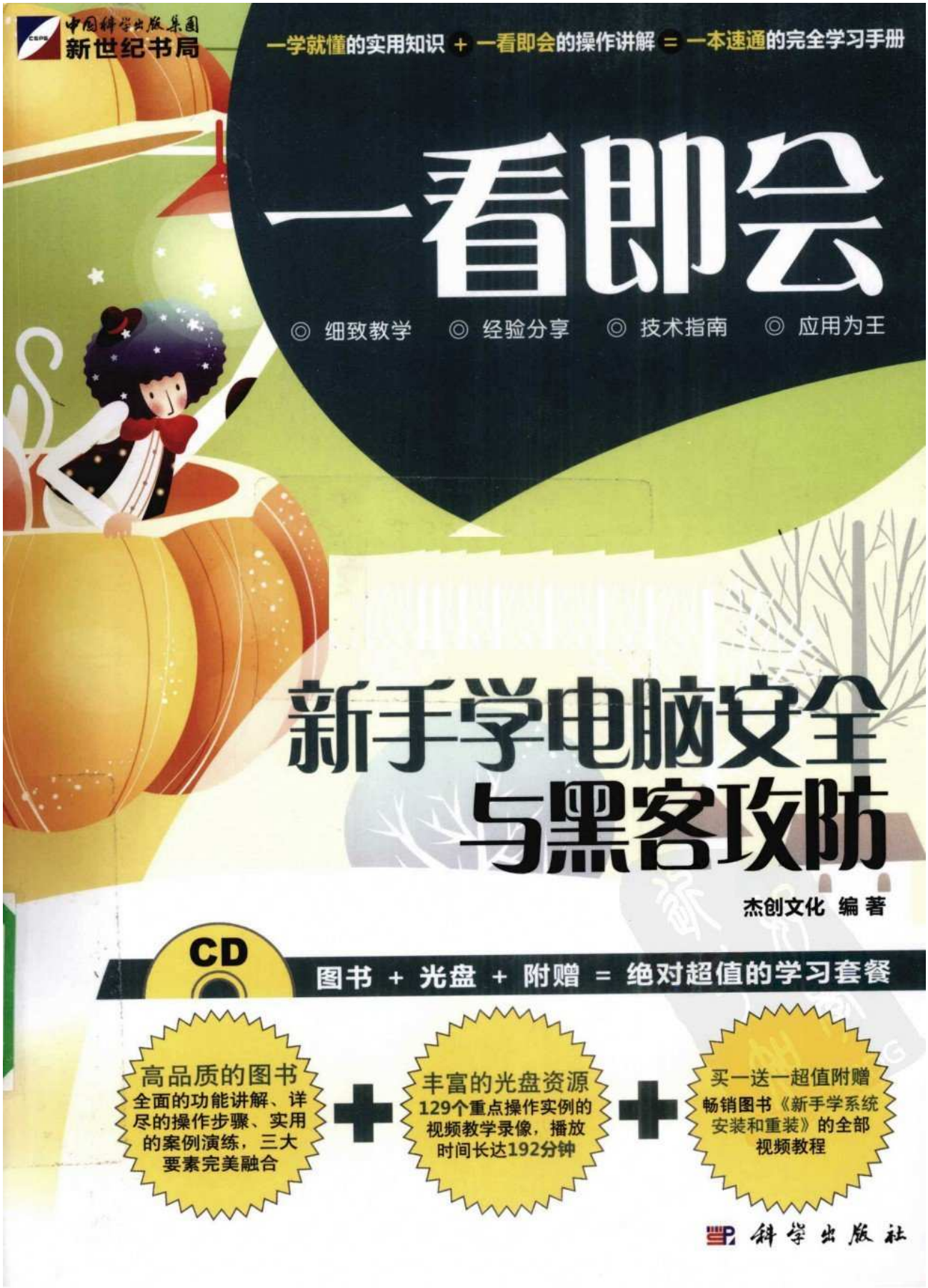


套书特色

- 专为初学者设计，选用最新行业知识和软件版本，科学安排知识体系、整理分享实用技巧、排困解难常见问题。
- 知识讲解由浅入深、循序渐进，辅以“新手学堂”与“提示”等内容，让读者更容易抓住重点、拓展应用。
- 选取融会所学知识、贴近实际应用、经过完整实测的精彩案例，Step by Step引导读者上手演练，立即检验学习成果。
- 多媒体光盘内容丰富，不仅包含对应书中知识体系的视频教程、实例文件，还超值加赠能进一步帮助读者提高应用水平的视频教程或软件。

一看即会

◎ 细致教学 ◎ 经验分享 ◎ 技术领先 ◎ 品质至上

出版服务信息
www.ncpress.com.cn

策　　划：中国科学出版集团新世纪书局
责任编辑：杨 倩　李 莉
封面设计：
技术支持：book@ncpress.com.cn
在线服务：www.ncpress.com.cn
直销电话：010 - 64869353

上架建议　计算机/网络技术/网络安全

ISBN 978-7-03-026948-5
9 787030 269485 >

定价：29.80元(含1CD价格)

前言 Preface

随着互联网技术的不断发展，信息交流更加高效、便捷，各种新的网络功能也不断涌现，网络在促进经济发展、推动社会进步和提高人们的生活质量等方面发挥着越来越重要的作用。然而与此同时，网络的安全问题也变得日趋严重，各种病毒、木马不断出现、花样还时时翻新，威胁着我们的电脑安全，需要引起每一个用户的重视。

此外，在网络中有一群被称为“黑客”的神秘人物。最早黑客是指热心于计算机技术、水平高超的电脑专家，尤指程序设计人员。但到了今天，黑客已被用于泛指那些专门利用电脑搞破坏或恶作剧的家伙。作为一个有一定操作经验的电脑用户，读者有必要了解一些黑客的知识，通过模拟黑客的行为准则以及入侵网络的方式、方法，反过来发现自身存在的问题，做好防范工作，从而最终保证自己的数据信息和网络财产的安全。

本书就是为读者量身打造的快速掌握电脑安全与黑客攻防技能的实用大全，全书共15章。第1章介绍电脑安全的基本知识，即为什么要注意电脑安全、电脑安全简介和常见的电脑安全技术等知识。第2章介绍如何为电脑设置密码，内容包括为电脑设置BIOS密码、账户密码，开启/关闭屏幕保护密码和电源管理密码，并且介绍了一些常用的密码设置技巧。第3~7章介绍了桌面、账户的安全设置，使用防火墙、修复系统漏洞，文件/文件夹及一些常用的软件的安全设置，备份与还原系统中的重要数据以及系统、上网过程中的一些安全操作等知识。第8章介绍在使用网上银行时应注意的一些问题以及安全操作等知识。第9章介绍关于病毒的基本知识，分别使用瑞星、金山毒霸和诺顿三种较为著名的杀毒软件查杀病毒及其相关设置等知识。第10章介绍黑客的基本知识，IP地址和端口的基本知识及分类，黑客常用的一些DOS命令及手段等知识。第11~15章介绍黑客常用的嗅探攻击以及怎样防范嗅探攻击，远程控制，QQ攻防、木马攻防以及电子邮箱攻防等知识。有了这些知识，你就能全面认识电脑的安全隐患和黑客的真实面貌，并掌握防范黑客入侵电脑的方法；就能了解常用的DOS指令以及对应的参数，尝试使用各种DOS指令；就能自己用杀毒软件查杀电脑中的病毒和木马啦。

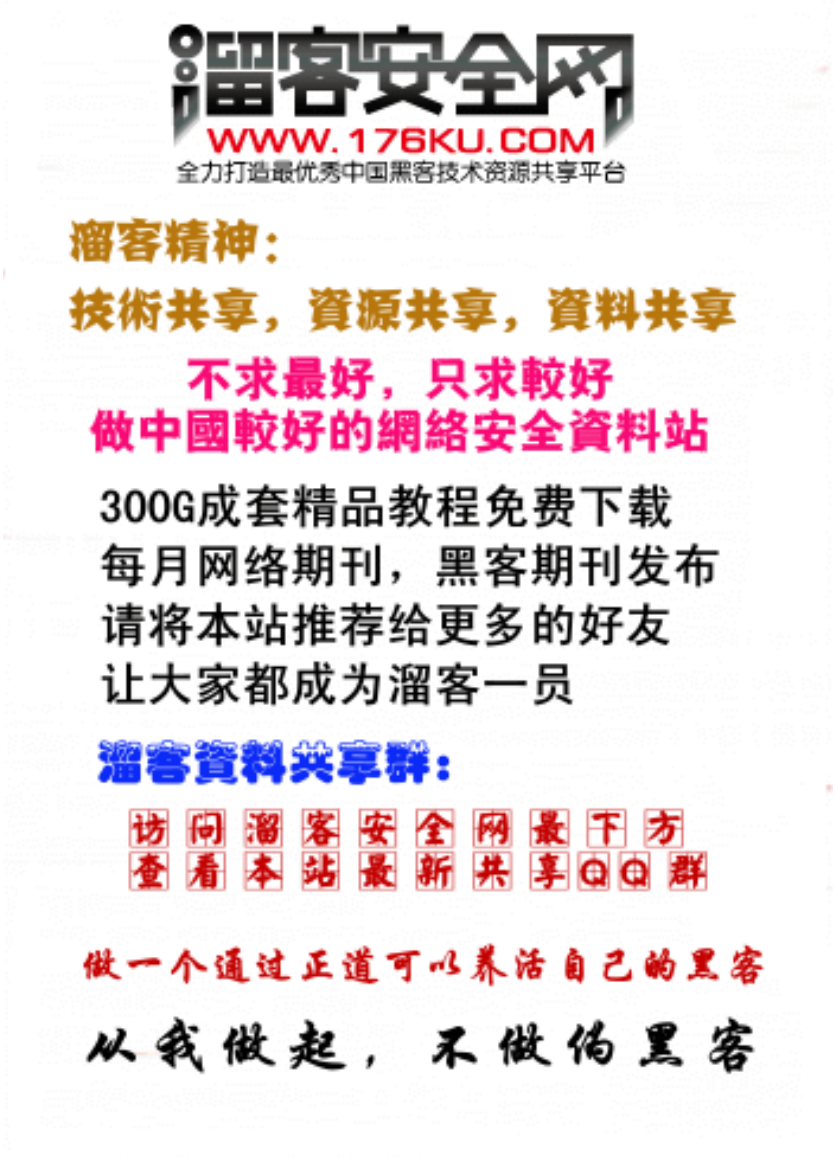
本书内容系统、全面，采用大量图片配合文字说明的方式对知识点进行介绍，步骤清晰、完备，保证读者一看即会！此外，在介绍操作方法时，尽量选用符合实际需求的实例，便于读者应用于实践。

本书配一张CD多媒体视频教学光盘，具有极高的学习价值和使用价值。光盘中包括播放时间长达192分钟的129个重点操作实例的视频教学录像，同时附赠了畅销图书《新手学系统安装和重装》的全部视频教程，具体使用方法请阅读下页的“多媒体光盘使用说明”。

本书由杰创文化组织编写。如果读者在使用本书时遇到问题，可以通过电子邮件与我们取得联系，邮箱地址为：1149360507@qq.com。此外，也可加本书服务专用QQ：1149360507与我们取得联系。由于作者水平有限，疏漏之处在所难免，恳请广大读者批评指正。

编著者

2010年3月



目录·Contents

Chapter 01

电脑安全入门

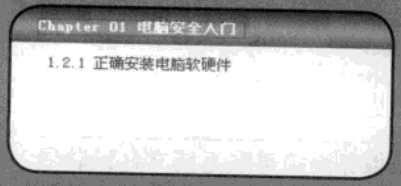
重点知识

1. 为什么要注意电脑安全
2. 电脑安全简介
3. 常见的电脑安全技术

随着科学技术的发展，电脑已经在社会生活的各个角落发挥了不同的作用，特别是互联网的推广与应用，使得人们的生活、工作、学习和交流环境逐渐发生改变，但是改变也有好有坏，好的会带来巨大的社会和经济效益，坏的则会使电脑存在危险性和脆弱性。为了能更好地使用和维护电脑，用户需首先了解电脑安全的基础知识以及常见的电脑安全技术。

视频文件

参见随书光盘：视频教程\Chapter 01



1.1 为什么要注意电脑安全

当用户使用电脑一段时间之后，许多安全问题就会不断地出现，常常出现的电脑安全问题包括误删除某些重要文件、黑客、电脑病毒和木马等。

电脑由硬件系统和软件系统组成，其中软件系统是相关的技术人员根据用户的需求进行编写的，所以在系统分析、系统设计等开发阶段中不可避免地会出现一些考虑不周的地方，对于某些大型的软件系统则很可能会出现一些软件漏洞，从而被黑客抓住漏洞进行攻击，造成电脑安全的问题，而有些电脑安全问题则是用户自己操作不当造成的，例如误删除某些重要文件而导致系统无法正常启动。下面介绍造成电脑安全问题的常见原因。

1 黑客

黑客，原意是指热心于电脑技术，水平很高的电脑专家，特别是程序设计人员，但是到了今天，黑客一词已被用于泛指那些专门利用电脑网络搞破坏或恶作剧的人。黑客通常利用操作系统或者某些软件的漏洞来入侵和控制电脑，以偷窥他人隐私、远程控制电脑、盗取他人的资料和账户密码等重要信息。所以用户应该及时修复系统漏洞并使用最新版本的应用软件。在修复系统漏洞时可开启电脑中的“自动更新”功能，或者登录微软官方网站手动下载并安装升级补丁。

“红客”一词来源于黑客，红色在中国有着特定的价值含义，即正义、道德、进步、强大，等等。红客是一种热爱祖国、坚持正义、开拓进取的精神，因此只要具备这种精神并热爱着电脑技术的人都可称为红客。

骇客同样来源于黑客，但是这类人专门使用恶意攻击、植入木马和病毒等一系列的破坏手段来破坏他人的系统，盗取他人的账号密码或者导致其他电脑系统彻底崩溃而丢失重要数据。

2 电脑病毒

电脑病毒是指编制或者在电脑程序中植入具有破坏功能或者毁坏数据，影响电脑使用，并能够自我复制的一组计算机指令或者程序代码。由于电脑病毒具有隐蔽性和突发性，当病毒入侵至电脑中时，一般会潜伏很长一段时间，一旦时机成熟就会对系统造成破坏，严重地影响电脑的安全。因此用户可以在电脑中安装杀毒软件，而病毒的种类在不断地增加，故用户需要及时升级杀毒软件并设置开机时启动实时保护。

3 木马

木马和病毒一样，也是一段电脑程序。但是木马和病毒有着不同的地方，木马是被用来盗取其他用户的个人信息或者诱导目标用户执行该程序以达到盗取密码等各种数据资料等目的。用户可使用杀毒软件扫描并查杀电脑中存在的木马。

4 误删除某些重要文件

普通用户一般对电脑中的某些重要文件不太认识，常常由于误操作而将某些系统文件删除导致无法启动系统，例如，有些用户为了方便，常常将应用软件安装到系统分区中，当需要手动删

除某些应用程序时，一不小心就很有可能将系统分区中的某些重要文件删除。为此，用户可将应用软件安装在除系统分区外的其他分区中。

1.2 电脑安全简介

电脑安全主要包括硬件和软件两方面的安全，安装电脑硬件时需要掌握正确的安装方法，安装软件也同样需要注意选择安装的路径和安装的附件。随着互联网的推广及应用，大量的电脑病毒、木马及黑客利用系统的漏洞或者用户的疏忽进入电脑并对电脑造成不同程度的损失，因此用户应了解电脑安全方面的知识，以阻止电脑病毒和黑客的入侵。

1.2.1 正确安装电脑软硬件

电脑硬件是用户使用电脑的基础，在正确安装之前需要了解电脑可以正常运行的环境。通常电脑要放置在一个干净、通风性比较好的办公环境中，而且要满足其运行所适宜的温度、湿度和电压等要求，以保证电脑硬件能够正常、高效地运行。除此之外，应该让电脑良好的接地，即接好家里的地线和购买好的插座板或者使用导线将机箱与地相连。当电脑中存放有重要数据时，应该安装屏蔽机房或者电子干扰设备。

1 安装多条内存条

内存是电脑系统运行过程中重要的临时信息场所，它是相对于外存而言的。用户平常使用的程序，如Windows操作系统、打字软件和游戏软件等，一般都是安装在硬盘等外存上的，但如果没有内存它们是无法工作的，必须把它们调入内存中运行才能使用。我们平时输入一段文字或者玩一个游戏，其实都是在内存中进行的，就好比在一个书房里，存放书籍的书架和书柜相当于电脑的外存，而我们工作的办公桌就是内存。通常我们把要永久保存的、大量的数据存储在外存上，而把一些临时的或少量的数据和程序放在内存上，当然，内存的好坏会直接影响电脑的运行速度。

若想要扩大内存容量可通过安装多条内存条来实现，在选购内存条的时候需要注意不同型号的内存条可能会因为速度问题产生一个时间差而导致电脑经常死机，建议用户在选购内存条时最好选择同种型号的内存条。由于内存的插槽在主板上，所以也要考虑到内存条与主板是否兼容的问题。在安装内存条时需要对准内存条的缺口与主板上内存插槽中的凸块，否则会损坏内存条或者内存插槽。

2 安装一个新的硬盘

电脑中的硬盘保存了操作系统、应用软件等重要的数据信息，一旦硬盘遭到破坏，硬盘中的数据将会遭受不同程度的破坏，给用户带来巨大的损失，因此用户必须正确地操作和使用硬盘。硬盘要远离磁场较强的环境，一般情况下硬盘都是固定在主机中，用户若要安装或者拆下硬盘时，要小心，不要摔打硬盘。

当硬盘的容量所剩无几时，用户就考虑到要在电脑中安装第二个硬盘，以IDE硬盘的安装为

例，用户在安装硬盘之前需要确定主机中是否有新增硬盘的安装空间，主机电源是否能满足新增硬盘的电源需求以及是否有空闲的硬盘插头。

满足以上三个条件之后，用户还需要在已安装主机机箱内的硬盘和新购买的硬盘之间选择引导系统的主盘，一般情况下选择已安装在主机机箱内的硬盘为主盘，新购买的硬盘为从盘。接着就可将硬盘连接在主板上对应的IDE接口中，一个IDE接口最多可接两个IDE设备，安装新硬盘之前，机箱主板上的IDE接口分别连接着光驱和安装了操作系统的硬盘，此时可将两个硬盘连接同一个IDE接口，连接之后就可开始设置跳线，跳线有三种设置，即master、slave和cable select，其中master是设置为主盘，slave是设置为从盘，cable select是根据在数据线上的位置自动决定主从盘关系。用户可按照硬盘说明书或者硬盘体上的详细说明进行跳线设置。设置完毕后将硬盘装入主机机箱中，然后连接好设备的数据线与电源线即可。

安装完成之后，两个硬盘很有可能会产生盘符交错的问题。当主硬盘中只有一个分区时便不会出现盘符交错的问题，而如果主硬盘中有至少两个分区时，就很有可能产生盘符交错，即将主硬盘的主分区默认为C盘，而新安装硬盘的主分区设置为D盘，然后依次排列主硬盘和新安装硬盘中的其他分区，这样一来就会导致除C盘以外的其他分区无法正常使用。用户有两种方法来解决该问题，一种方法是对新安装的硬盘进行重新分区，并且在分区的过程中将所有分区都设置成扩展分区；另一种方法是在BIOS设置界面中的“Standard CMOS Features”选项中将第二硬盘的IDE设置为None。

3 正确放置显示器

在使用完电脑之后应当关闭显示器。由于现在大多数的显示器都具有DPMS（显示器电源管理）功能，即在主机关闭之后，显示器能够长时间保持节能方式，但是长时间使显示器处于开启状态会使显示器的消磁电路无法对显示器进行消磁处理，从而使显示器屏幕因长期得不到消磁而造成偏色现象。

在使用显示器时，应尽量让其处在通风性较好的位置并且还要注意防潮。显示器正在运行时不要遮住其通风孔并且不要在上方放置任何东西，否则会因无法散热而造成显示器内温度过高；在放置显示器时应尽量使其保持平衡，不要放在沙发、床等比较软的物体上；若放置显示器的环境比较潮湿，需要做好防潮措施，即在显示器旁放置一个风扇或者食品包装袋中的防潮剂。不能将水或者其他液体滴入显示器内，否则会影响显示器的正常工作或者损坏显示器；不要用带有腐蚀性或者导电性液体的布料品擦拭显示器屏幕，只能用较干的布或者专用的电脑清洗剂来擦拭，并且在擦拭之前一定要确保电脑处于关闭状态，为了安全，建议用户切断电源。

4 正确使用USB可移动设备

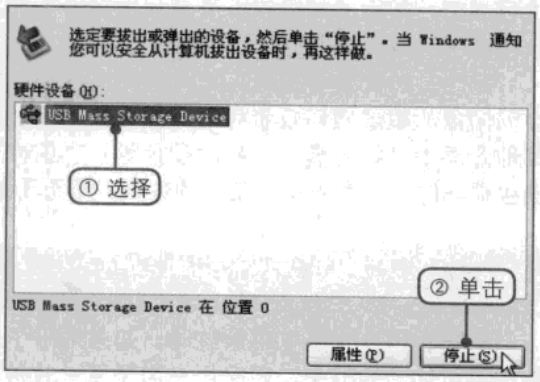
USB的全称是Universal Serial Bus，中文含义是“通用串行总线”。USB是一个外部总线标准，用于规范电脑与外部设备的连接和通信。USB接口支持设备的即插即用和热插拔功能。而USB接口的移动硬盘不仅容量大，而且携带方便，用户在携带或者使用时不要损坏该设备，否则将会导致该移动硬盘内的数据无法读出或者根本无法识别。另外，用户在使用移动硬盘时，直接将其连线与机箱的USB接口相连接即可，系统会自动检测到新硬件并识别。USB接口虽然支持热插拔，但是建议用户在取走移动硬盘时按照如下的步骤进行。

① 单击“安全删除硬件”命令

当用户想要安全取走移动硬盘时，①在桌面上的通知区域中右击图标。②在弹出的菜单中单击“安全删除硬件”命令。

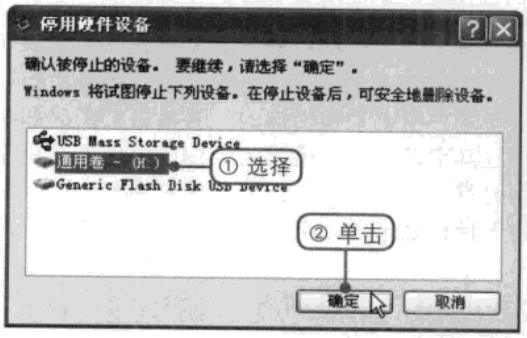
② 选择要拔出的设备

弹出“安全删除硬件”对话框，①在硬件设备中选择USB Mass Storage Device选项。②单击“停止”按钮。



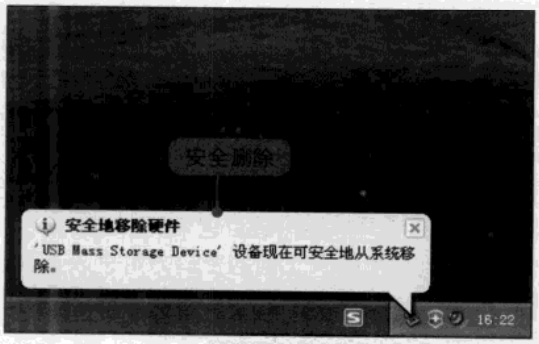
③ 停用硬件设备

弹出“停用硬件设备”对话框，①在列表框中选择“通用卷－（H：）”选项。②单击“确定”按钮。



④ 安全删除

此时在桌面右下角的通知区域中即可看见“安全地移除硬件”提示信息。



5 正确安装应用软件

用户不仅要能正确地安装某些硬件，而且也要掌握安装应用软件的技巧。如果需要在网站上下载安装软件，那么在选择下载网站时，一般都是直接登录该软件对应的官方网站进行下载，若登录其他网站有可能会下载到带有病毒或者木马的安装软件。成功下载安全的安装软件后，在安装时也要注意技巧，有些安装软件会带有一些附加的软件使其一起安装，例如在安装某些应用软件时会询问用户是否安装Google工具栏，若不仔细就直接将其安装至电脑中了，所以在安装软件过程中需要看清楚后再操作，一般建议用户将应用软件安装在除系统分区之外的其他分区中，否则当用户重装系统后系统分区中的应用软件都会被格式化。

1.2.2 对重要数据要多重保护

电脑中的数据一般都存放在硬盘中，其中也包括重要的数据，将重要数据存放到硬盘后，需要对这些数据做好多重保护。可直接在“我的电脑”窗口中将其隐藏；若觉得该种隐藏法不够安全，则可以使用WinRAR压缩软件将重要数据进行加密压缩；也可以使用第三方软件对重要数据进行加密，常用的加密软件有高强度文件夹加密大师和万能加密器。加密之后用户也可使用操作系统自带的备份工具将重要数据进行备份。

无论是加密或者备份，其对应的文件都是放置在硬盘中，但是硬盘并不是完全安全的，可能会因硬盘的磁道损坏或者病毒入侵等原因而造成重要数据的丢失。因此用户可将重要数据存储到其他介质中（如光盘、可移动硬盘等），这样一来就可确保重要数据的安全性，当电脑中的数据发生损坏时，可直接使用备用的数据，不至于造成很大的损失。

1.2.3 保障系统安全

当非法用户入侵电脑系统时，如果做好了系统的安全措施则不会造成很大的损失，否则将会造成不可估计的损失，因此用户需要通过各种措施来保障系统的安全，例如为系统设置不同的密码、对系统的安全进行相关的设置、及时修复系统漏洞等。

1 为系统设置密码

用户可以在系统设置BIOS密码、账户密码、屏幕保护密码和电源管理密码。BIOS密码是用来防止非法用户进入BIOS并肆意篡改其设置的，在BIOS密码中又可分为普通用户密码和超级用户密码，使用普通用户密码进入BIOS设置界面后，只能查看和浏览其相关设置，并不能设置其中的某些重要属性，而使用超级用户密码进入BIOS设置界面后，不但能够查看和浏览相关设置，而且还可以对BIOS的所有属性进行更改；账户密码则是为了防止非法用户进入桌面后对系统进行盗取或者破坏操作；屏幕保护密码和电源管理密码均是与账户密码紧密相连的，屏幕保护密码和电源管理密码只有在设置了账户密码的情况下有效，并且其密码与账户密码完全相同，只是适用于不同的情况，屏幕保护密码适用于用户暂时离开电脑的那一段时间，防止非法用户偷窥电脑，液晶显示器使用屏幕保护是百害而无一利的；当电脑处于待机状态时，电源管理密码即可生效，再次启动时则需要输入正确的密码方可进入桌面。

2 设置系统安全

当一台电脑并非一个人使用时，就需要在操作系统中建立一些除管理员账户外的其他账户，而Windows系统拥有比较完善的系统用户权限管理功能，用户可以以管理员的身份创建各个权限不同的账户，这样其他用户就无法访问系统中一些特定的数据或者文件，从而保证了特定数据的相对安全。用户可在桌面上进行一系列的安全设置，例如隐藏通知区域中的程序图标、自动隐藏任务栏、快速隐藏桌面程序图标或者隐藏“屏幕保护程序”选项卡等。为了进一步的安全，用户可进入本地安全策略中设置账户策略和本地策略，用户还需要开启并配置Windows防火墙或者使用其他防火墙来保护系统，如天网防火墙。

3 修复系统漏洞

当选择了一款操作系统时，该操作系统不可避免地存在一些漏洞，一些黑客往往会利用这些

漏洞来攻击电脑，向电脑植入木马或者病毒，所以应及时修复系统漏洞，如开启Windows自动更新、登录微软官方网站下载并安装升级补丁或者使用第三方软件自动修复系统漏洞，常用的第三方软件包括360安全卫士和超级兔子。

4 系统备份与还原

在做好系统的安全措施并成功修复漏洞之后，就可以使用系统自带的备份工具备份系统或者使用一键GHOST、一键还原精灵备份系统，当系统出现问题时可直接将备份的文件还原，使系统恢复到备份时的状态。

>> 1.2.4 谨慎上网

随着互联网的发展及推广，越来越多的电脑与互联网相连接，从而实现了与互联网上其他电脑的信息共享。但是用户在通过互联网获得利益的同时，也要防止网络中不安全因素的入侵，需谨慎上网。

电脑网络存在许多的安全问题，有些可能是用户自己造成的，例如账户密码设置过于简单、将自己的账户随意借给他人或者与他人共享等；有些则可能是黑客利用系统漏洞对电脑进行攻击而造成的，当攻击成功之后就可轻易地盗取电脑上的重要信息、账户和密码等。

1 设置浏览器

由于用户浏览网页都是通过浏览器来进行的，因此在连接互联网之后需要设置浏览器的安全，例如设置浏览器的安全级别、设置受信任站点和受限站点以及阻止弹出窗口等，当浏览器遭到破坏时，可通过一些浏览器修复软件修复，如使用IE浏览器修复工具修复IE浏览器等。

2 不要打开不知名的网页

在浏览网页时需要特别注意，某些不知名的网页很有可能携带有病毒或者木马，一旦用户打开该类网页，网页携带的病毒或者木马就会入侵电脑，所以用户在浏览网页时尽量浏览自己熟悉的网页或者通过百度、Google等搜索引擎网站进行搜索。

1.3 常见的电脑安全技术

为了使电脑资源能够正常稳定地运行，并使用户受控、合法地使用电脑信息。用户在了解了电脑安全的相关知识之后，需要掌握常见的电脑安全技术，包括安全设置密码，电子邮件安全、IE浏览器安全和定期升级系统等技术。

常见的电脑安全技术如下。

1 安全设置密码

在设置密码时不要简单地用生日、单词或电话号码作为密码，密码的长度至少要8个字符以上，包含数字、大/小写字母和键盘上的其他字符混合。对于不同的网站和程序，要使用不同口令，以防止被黑客破译。要记录好ID和密码以免忘记，但不要将其记录在上网的电脑里。而且还要经常更改密码，不要向任何人透露您的密码。

2 电子邮件安全

在不知道信息来源的情况下，不要轻易打开电子邮件中的附件，更不要轻易运行。要时刻保持警惕性，不要轻易相信熟人发来的E-mail就一定没有黑客程序，不要在网络上随意公布或者留下自己的电子邮件地址，可以去转信站申请一个转信信箱，对于邮件附件要先用防病毒软件和专业清除木马的工具进行扫描后方可使用。

3 IE浏览器安全

对于使用公共电脑上网的用户，一定要注意IE的安全性。因为IE的自动完成功能在给用户填写表单和输入Web地址带来一定便利的同时，也给用户带来了潜在的泄漏危险，最好禁用IE的自动完成功能。IE的历史记录中保存了已经访问过的所有页面的链接，在离开之前一定要清除历史记录；另外IE的临时文件夹内保存了用户已经浏览过的网页，通过IE的脱机浏览特性或者是其他第三方的离线浏览软件，其他用户能够轻松地翻阅你浏览的内容，所以在离开之前也需删除该路径下的文件。还要使用能够控制Cookie程序的安全程序，因为Cookie能够存储用户在特定网站上的密码和ID并且把信息传回网站。安装个人防火墙可对Cookie的使用进行禁止、提示或启用。

4 防止木马

不要轻易安装和运行从不知名的网站（特别是不可靠的FTP站点）下载的软件和来历不明的软件。有些程序可能是木马程序，一旦安装了这些程序，它们就会在用户不知情的情况下更改系统或者连接到远程的服务器。这样，黑客就可以很容易进入电脑。另外，如果购买二手电脑，则不要购买或者使用那些曾经遭受过黑客入侵，但仍未清理过硬盘的二手电脑，因为这样很可能会为黑客再次提供入侵电脑的机会，最好是重新格式化硬盘，并重装操作系统。

5 定期升级系统

很多常用程序和操作系统的内核都会发现漏洞，某些漏洞会让入侵者很容易进入到用户的系统，这些漏洞将会以很快的速度在黑客中传开，因此一定要小心防范。软件的开发商会把补丁公布，以便用户补救这些漏洞。建议用户订阅关于这些漏洞的邮件列表，以便及时修复漏洞以防黑客攻击。还可以使用最新版本的浏览器软件、电子邮件软件以及其他程序，但不要是测试版本。

6 安装防火墙

不要在没有防火墙的情况下上网。如果使用的是宽带连接，如ADSL或者光纤，那么电脑会在任何时候都连上Internet，这样，该电脑就很有可能成为一些黑客的攻击目标。最好在不需要的时候断开连接，例如可以在电脑上装有防黑客的防火墙——一种反入侵的程序作为电脑的门卫，以监视数据流动或是断开网络连接。如Lockdown2000 、ZoneAlarm、天网或者其他的一些个人防火墙软件。另外，如瑞星、江民、金山公司的最新版杀毒软件都附有防火墙，可以起到杀毒、防黑的双重功效。

7 禁止文件共享

局域网里的用户喜欢将自己的电脑设置为文件共享，以方便相互之间资源共享，但是在设置了共享之后，就为黑客留了后门，这样他们就可趁机进入电脑偷窥文件，甚至破坏系统。建议用户在非设共享不可的情况下，最好为共享文件夹设置一个密码，否则公众以及你的对手将可以自由地访问那些共享文件了。

Chapter 02

为电脑设置密码

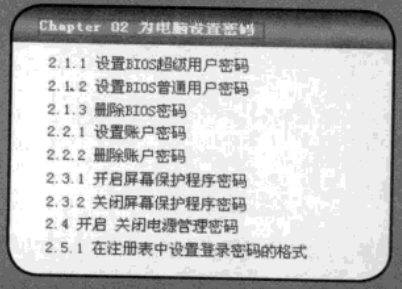
重点知识

1. BIOS密码
2. 账户密码
3. 屏幕保护程序密码
4. 电源管理密码
5. 密码设置技巧

用户成功启动电脑之后，可以通过为其设置密码来保障电脑的安全，如设置BIOS密码可防止非法用户肆意篡改BIOS中的相关信息；设置账户密码可以防止非法用户登录电脑桌面。除了这两种密码之外还可以设置屏幕保护密码和电源管理密码。用户在设置密码时可以通过注册表来设置登录密码的格式并掌握一些设置密码的技巧。

视频文件

参见随书光盘：视频教程\Chapter 02



2.1 BIOS密码

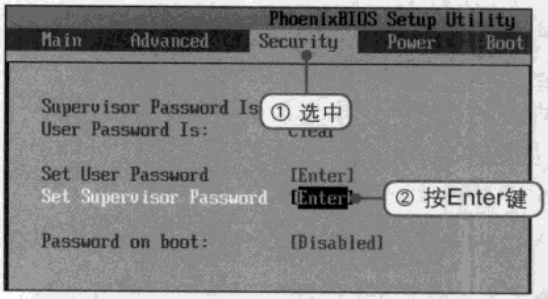
BIOS是英文Basic Input Output System的缩略语，译成中文名是“基本输入输出系统”。BIOS保存着电脑中最重要的基本输入输出程序、系统设置信息、开机后自检程序和系统自启动程序。可以在BIOS界面中设置密码以防止其他用户修改BIOS中的重要设置。若不需要该密码时也可在BIOS界面上将其直接删除。

2.1.1 设置BIOS超级用户密码

可以根据主板说明书上介绍的方法进入BIOS界面，然后在BIOS界面中设置超级用户密码。使用BIOS超级用户密码的用户不仅可以正常启动电脑中的各类软件，而且可以进入BIOS界面对部分选项进行修改和设置。

① 选中Security选项

①进入BIOS界面后使用键盘上的方向键选中Security选项。②此时光标固定在Set Supervisor Password选项上，按Enter键。

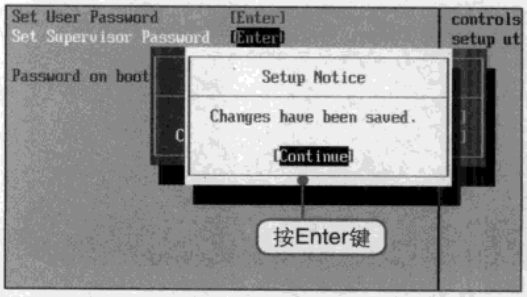


② 输入密码

弹出Set Supervisor Password对话框，在Enter New Password输入框中输入密码后按Enter键后再次输入相同的密码。

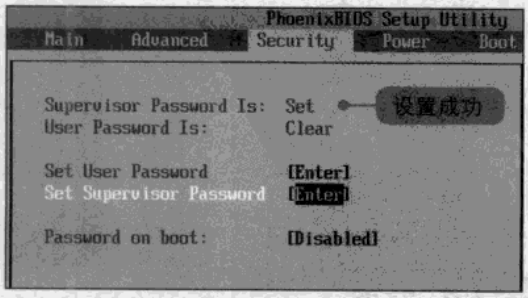
③ 确定设置的密码

按Enter键后弹出Setup Notice对话框，此时光标固定在Continue选项上，直接按Enter键。



④ 成功设置超级用户密码

可以看见Supervisor Password Is选项是Set状态，即超级用户密码设置成功。



2.1.2 设置BIOS普通用户密码

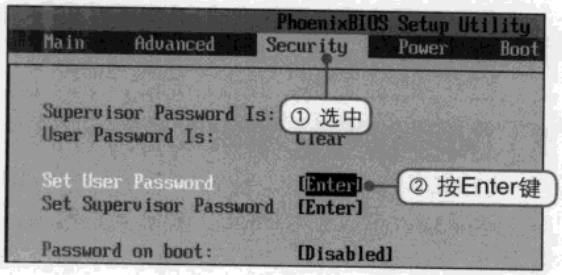
使用BIOS普通用户密码的用户虽然可以正常运行电脑中的各类软件，也能够进入并浏览BIOS设置界面，但是却不能更改其中的任何设置。

① 输入超级用户密码

进入BIOS界面，系统要求用户输入超级密码，然后按Enter键即可进入BIOS界面。

② 选中Security选项

①使用键盘上的方向键选中Security选项。②光标固定在Set User Password选项上，按Enter键。



③ 设置密码

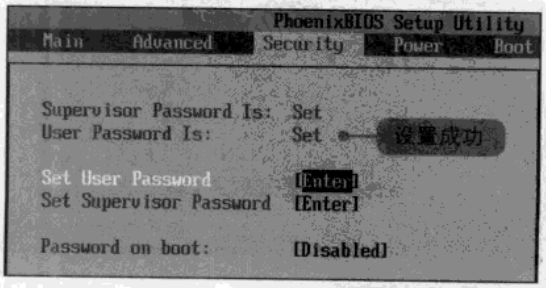
弹出Set User Password对话框，在Enter New Password输入框中输入密码后按Enter键后再次输入相同的密码。

④ 确认输入的密码

按Enter键后弹出Setup Notice对话框，光标固定在Continue选项上，按Enter键。

⑤ 成功设置普通用户密码

此时可以看见User Password Is选项是Set状态，即普通用户密码设置成功。



使用普通用户密码进入BIOS界面后无法设置的选项

提示

使用普通用户密码进入BIOS界面后，Advanced和Boot选项卡下的大部分选项呈现灰色，无法手动设置。但是在Main选项卡下可以手动设置时间和日期，并且可以修改设置的普通用户密码。

2.1.3 删除BIOS密码

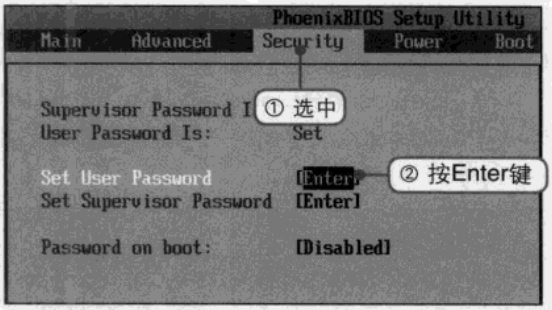
用户也可按照前面的方法在BOIS界面的Security选项下删除设置的BIOS超级用户密码和普通用户密码。

① 输入超级用户密码

进入BIOS界面后，系统要求用户输入密码，这里输入可以设置BIOS的超级用户密码，接着按Enter键即可进入BIOS界面。

② 选中Security选项

①使用键盘上的方向键选中Security选项。②使用方向键选择Set User Password选项并按Enter键。



③ 输入原始的普通用户密码

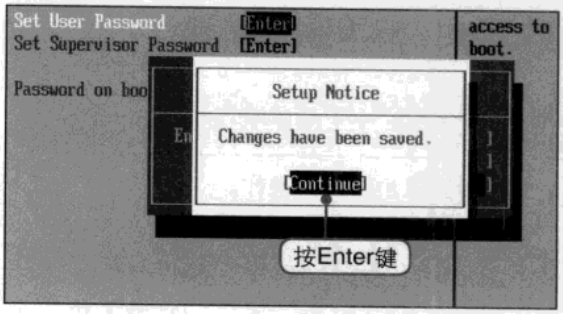
弹出Set User Password对话框，在Enter Current Password输入框中输入原始的普通用户密码并按Enter键。

④ 删除密码

光标跳至Enter New Password输入框中，直接按Enter键后光标跳至Confirm New Password选项，继续按Enter键。

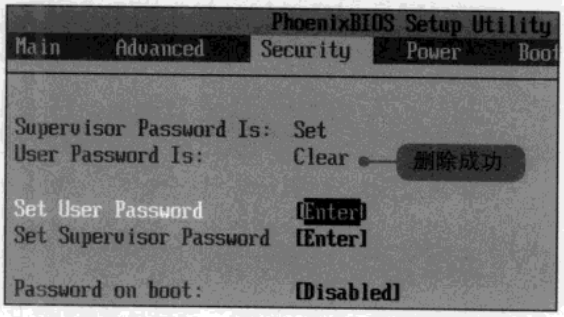
⑤ 确认删除密码

弹出Setup Notice对话框，提示用户更改已经保存，此时光标固定在Continue选项上，按Enter键。



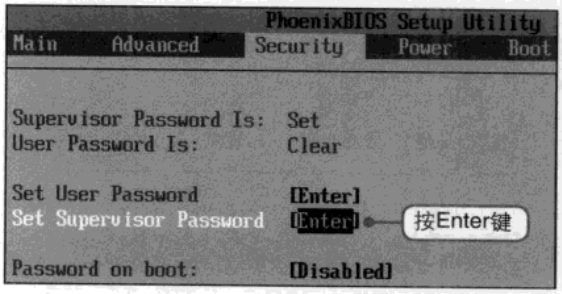
⑥ 删除成功

此时可在BIOS界面中看见User Password Is选项是Clear状态，即普通用户密码成功被删除。



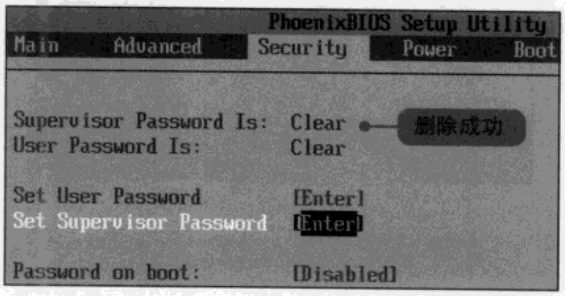
⑦ 删除超级用户密码

接着使用方向键将光标移至Set Supervisor Password选项上，然后按Enter键。



⑧ 成功删除超级用户密码

同样的方法删除超级用户密码，删除后Supervisor Password Is呈现Clear状态。



忘记了BIOS密码怎么办

■ **使用跳线短路法**

在主板使用说明书上找到清除CMOS数据的跳线位置，然后将该组跳线短路至少6秒以上即可清除CMOS中存储的所有数据。

■ **将主板电池放电**

将电源插头拔掉，接着将主机内银白色的纽扣电池取下约10分钟后再将电池装上，重启后系统提示CMOS在检查时发现了错误，自动载入了系统的默认值。

2.2 账户密码

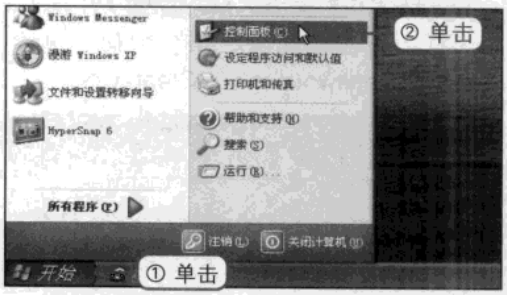
账户密码可以防止非法用户进入电脑桌面。用户可在控制面板的“用户账户”界面中设置账户密码，成功设置之后用户每次进入系统桌面之前都要输入有效的账户密码，必要时也可以删除账户密码。

2.2.1 设置账户密码

可以通过控制面板打开“用户账户”界面，然后进行设置账户密码的操作。

① 删除超级用户密码

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“控制面板”命令。

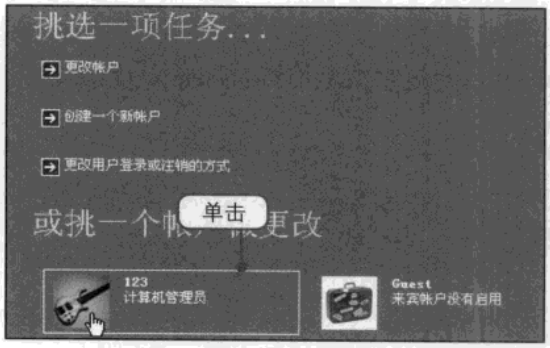


② 双击“用户账户”图标

打开“控制面板”窗口，双击“用户账户”图标。

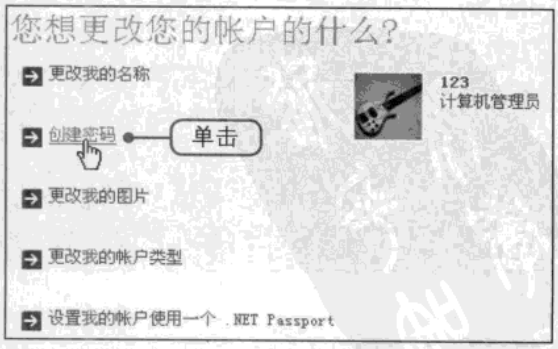
③ 选中需要设置密码的账户

打开“用户账户”窗口，在“或挑一个账户做更改”选项组中单击需要设置密码的账户，例如单击“计算机管理员”。



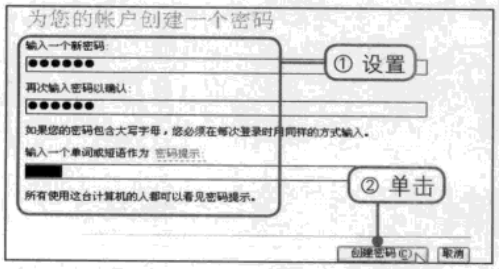
④ 单击“创建密码”文字链接

打开“您想更改您的账户的什么”界面，单击 “创建密码”文字链接。



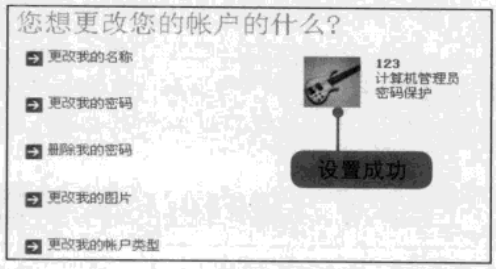
⑤ 设置账户密码

打开“为您的账户创建一个密码”界面，①依次输入两次密码和密码提示。②单击“创建密码”按钮。



⑥ 成功设置账户密码

返回“您想更改您的账户的什么”界面，此时可在界面中看见“计算机管理员密码保护”等字幕，即账户密码设置成功。

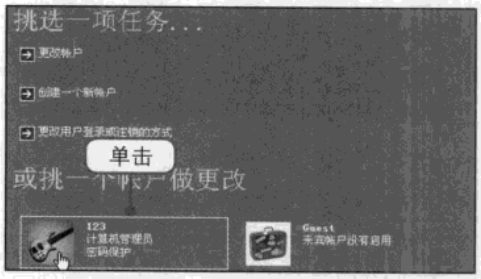


2.2.2 删除账户密码

若想要删除所设置的账户密码，同样可以在“用户账户”窗口中完成该操作。

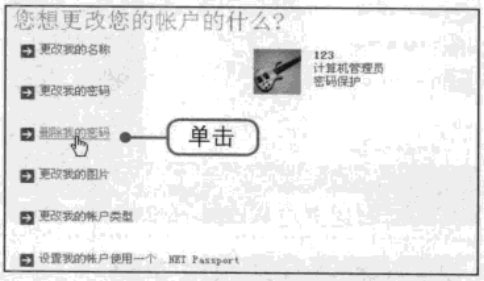
① 选中需要删除密码的账户

按照前面的方法打开“用户账户”窗口，单击需要删除密码的账户。



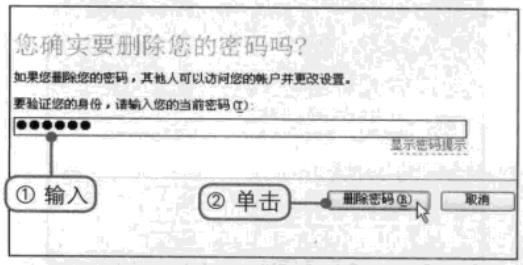
② 单击“删除我的密码”文字链接

打开“您想更改您的账户的什么”界面，单击“删除我的密码”文字链接。



③ 删除密码

打开“您确实要删除您的密码吗？”界面，①在下方的文本框中输入原始密码。②单击“删除密码”按钮。



④ 成功删除账户密码

返回“您想更改您的账户的什么”界面，用户可看见界面中出现了“创建密码”的字样，则账户密码成功删除。

2.3 屏幕保护程序密码

屏幕保护程序常用于纯平显示器，它具有延长显示器的使用寿命和省电等作用。当用户使用笔记本或者液晶显示器时，因为液晶显示器的工作原理和纯平显示器的工作原理不一样，因此使用屏幕保护程序将会对液晶显示屏造成伤害。但是无论液晶显示器或者纯屏显示器均可开启屏幕保护程序密码，屏幕保护程序密码可以防止在用户暂时离开电脑的那段时间内其他用户偷窥电脑上的一些隐私。

2.3.1 开启屏幕保护程序密码

屏幕保护程序的密码与当前账户的账户密码完全一致，即屏幕保护密码生效的前提是当前账户必须设置账户密码。可通过“控制面板”打开“显示 属性”对话框，在该对话框中开启屏幕保护程序密码。

① 打开“控制面板”窗口

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“控制面板”命令，打开“控制面板”窗口。

② 打开“显示”对话框

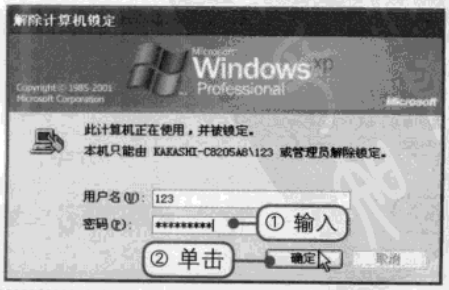
在“控制面板”窗口中双击“显示”图标，打开“显示 属性”对话框。

③ 开启屏幕保护程序密码

①在“显示 属性”对话框中单击“屏幕保护程序”标签切换至该选项卡。②勾选“在恢复时使用密码保护”复选框。

④ 成功开启

单击“确定”按钮关闭对话框即设置成功。当用户离开电脑一段时间后再次使用电脑时，①在弹出的“解除计算机锁定”对话框中输入密码。②单击“确定”按钮即可进入桌面。

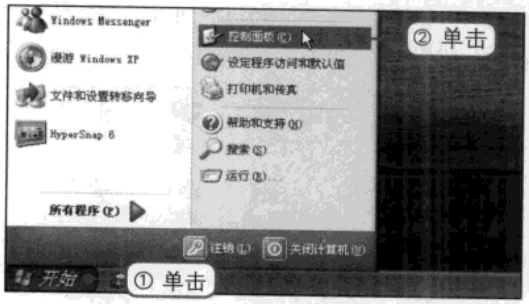


2.3.2 关闭屏幕保护程序密码

若用户需要关闭屏幕保护程序密码则可在“显示 属性”对话框中取消勾选“在恢复时使用密码保护”复选框即可。

① 打开“控制面板”窗口

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“控制面板”命令，打开“控制面板”窗口。



② 打开“显示”对话框

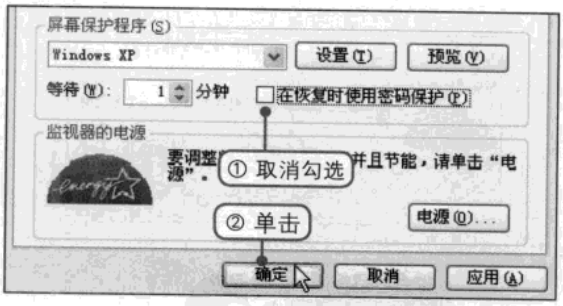
在“控制面板”窗口中双击“显示”图标，打开“显示”对话框。

③ 切换至“屏幕保护程序”选项卡

在“显示 属性”对话框中单击“屏幕保护程序”标签切换至该选项卡。

④ 关闭屏幕保护程序密码

①取消勾选“在恢复时使用密码保护”复选框。②单击“确定”按钮保存退出。



不同的显示器要有不同的保养方法

有些用户喜欢使用精美和色彩变幻的屏幕保护程序，其实这种屏保对于电脑硬件来说却加重了它们的工作负荷，对于使用电池供电的笔记本来说则是加快了电量的消耗。在一段时间内离开液晶显示器的电脑或笔记本电脑时，最好关闭显示器或者使其处于待机状态；笔记本可直接扣下屏幕，则系统自动处于待机状态，回来时掀起屏幕可继续工作。

2.4 开启/关闭电源管理密码

电源管理密码与当前账户的账户密码一致，其主要作用与屏幕保护密码差不多，但是电源管理密码是电脑从待机状态苏醒后进入桌面前必须输入的密码。可通过“显示 属性”对话框来开启或者关闭电源管理密码。

① 单击“控制面板”命令

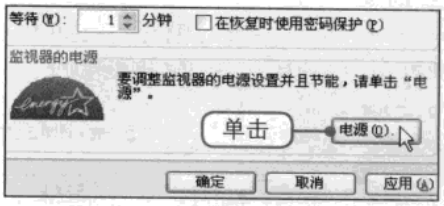
①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“控制面板”命令。

② 打开“显示 属性”对话框

在“控制面板”窗口中双击“显示”图标，打开“显示 属性”对话框。

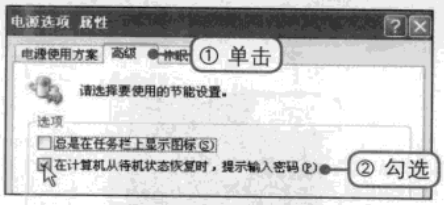
③ 单击“电源”按钮

在“屏幕保护程序”选项卡中单击 “电源”按钮，打开“电源选项 属性”对话框。



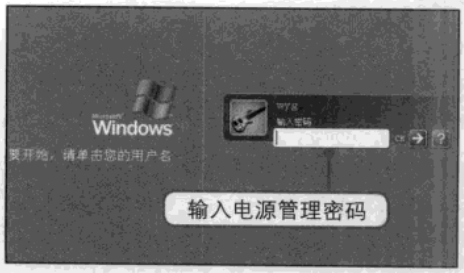
④ 开启电源管理密码

①单击“高级”标签切换至该选项卡。②勾选“在计算机从待机状态恢复时，提示输入密码”复选框。然后单击“确定”按钮。



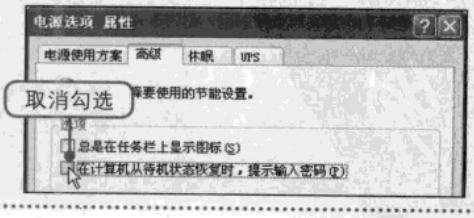
⑤ 成功开启电源管理密码

当电脑从待机状态苏醒后，此时系统要求用户必须输入有效的电源管理密码方可进入桌面。



⑥ 关闭电源管理密码

若用户不想使用该密码时，按照前面的操作步骤打开“电源选项 属性”对话框，取消勾选“在计算机从待机状态恢复时，提示输入密码”复选框即可。



2.5 密码设置技巧

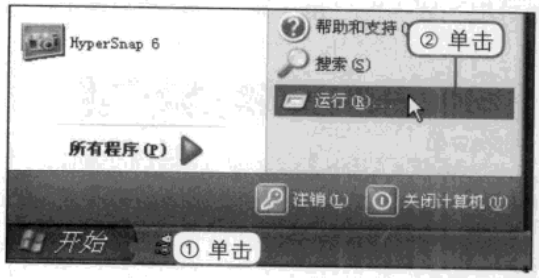
在设置BIOS密码或者账户密码时必须要掌握一些设置密码的技巧，例如用户可在注册表中设置登录密码的格式，以限制密码的某些属性，如长度或者组成等。除此之外，用户也需要掌握一些设置密码常用的技巧，如设置的密码不能太短等。

2.5.1 在注册表中设置登录密码的格式

在设置密码之前可以通过注册表设置登录密码的格式，例如在注册表中可设置密码的最小长度、限制密码仅由数字和字母组成等。

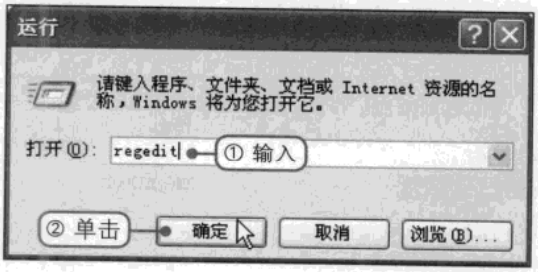
① 打开“运行”对话框

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“运行”命令，打开“运行”对话框。



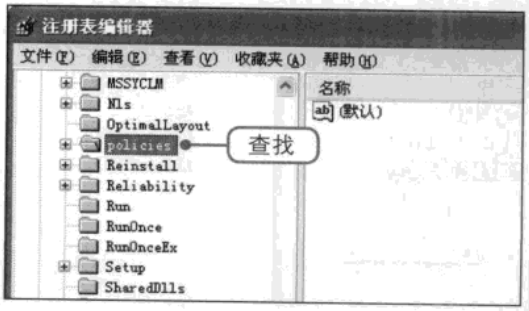
② 打开“注册表编辑器”窗口

①在“运行”对话框中的“打开”文本框中输入regedit指令。②单击下方的“确定”按钮。



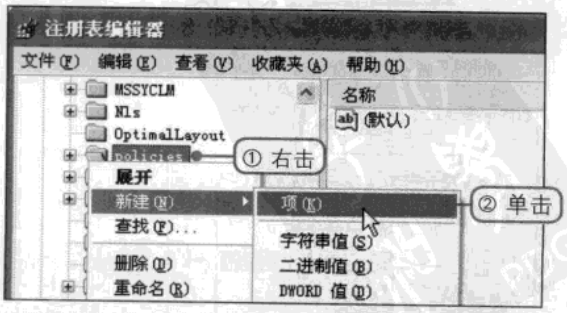
③ 查找policies选项

从“注册表编辑器”窗口的左侧栏中依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion选项，在Current Version选项下查找policies选项。



④ 新建子项

①右击policies选项。②在弹出的快捷菜单中单击“新建>项”命令，新建一个子项。

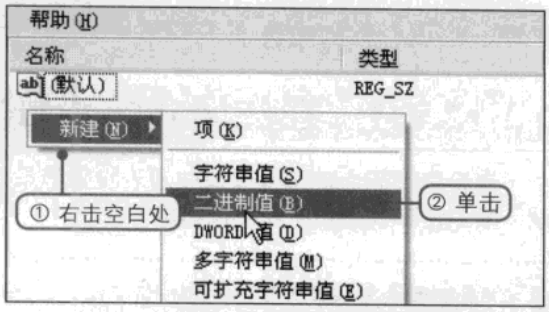


5 重命名为Network

新建子项名处于可编写状态，将新建的子项重命名为Network，接着按Enter键。

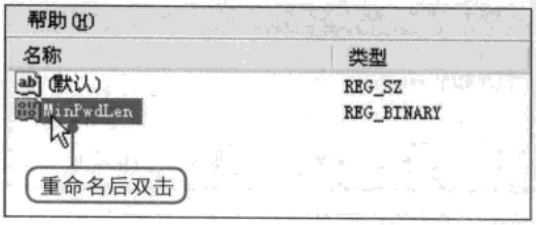
6 新建一个二进制值

选中Network选项，①右击窗口右侧的空白处。②在弹出的快捷菜单中单击“新建>二进制值”命令，新建一个二进制值。



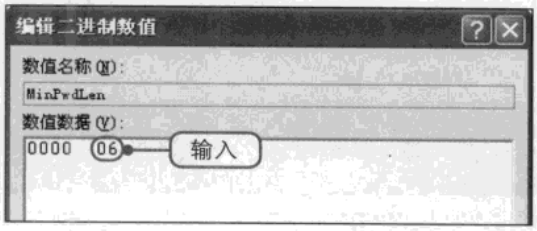
7 重命名为MinPwdLen

新建的二进制值名处于可编写状态，将其重命名为MinPwdLen并按Enter键，接着双击该选项。



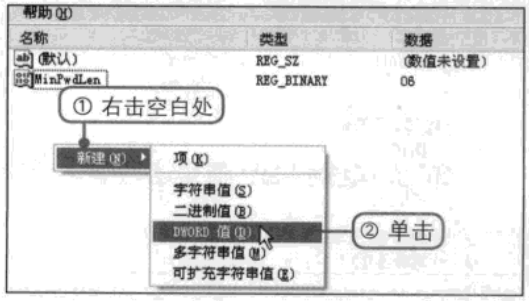
8 编辑二进制数值

弹出“编辑二进制数值”对话框，在“数值数据”列表框中输入06，表示密码的最小长度为6位，然后单击“确定”按钮。



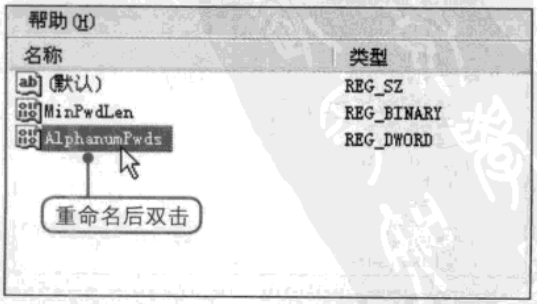
9 新建DWORD值

返回“注册表编辑器”窗口，此时可以看见MinPwdLen选项的数据为06，①右击空白处。②在弹出的快捷菜单中单击“新建>DWORD值”命令。



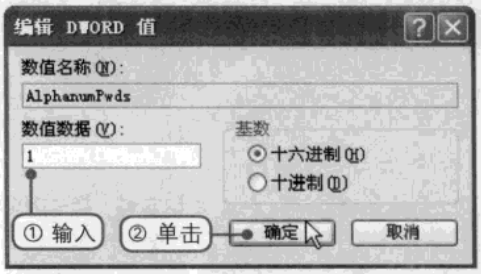
10 重命名为AlphanumPwds

此时DWORD值选项名处于可编写状态，将其重命名为AlphanumPwds并按Enter键。然后双击该选项，弹出“编辑DWORD值”对话框。



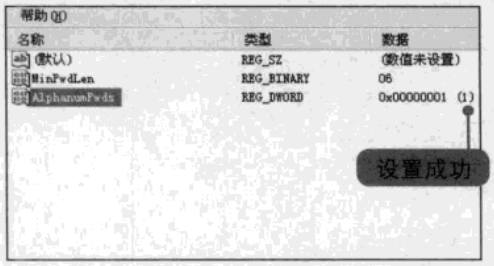
11 设置数值数据

在对话框中的“数值数据”文本框中输入1，表示以后设置的密码就只能由数字和字母组成，然后单击“确定”按钮。



12 设置成功

返回“注册表编辑器”窗口，此时可在窗口右侧看见AlphanumPwds选项的数值属性为1。



2.5.2 常用的设置技巧

用户除了在注册表中设置登录密码的格式之外，还必须掌握一些常用的设置技巧。

- 密码的位数至少要设置6位，并且设置密码时要使密码中含有大/小写字母、标点和数字等符号。
- 不要以所有单词、生日、数字和手机号码作为密码，这种密码很容易被破解。例如将生日作为密码，如果是出生在20世纪，即19××年，而一年有12个月，每个月最多只有31天，因此破解这种密码只需要几分钟。
- 密码中的英文可以混合使用大写字母和小写字母。
- 在程序允许的情况下，密码中可以添加英文半角的符号。
- 不要用a、b、c等比较靠前字母表的字母或者数字开头，由于字典暴力破解的程序一般都是从数字或者英文字母排序开始算的。
- 设置“无规律”的密码。这种无规律是针对除用户之外的其他人，但是对于用户来说，这种密码的联系要很隐蔽。例如用户若想使用kakashi1987作为密码，则可以设置成xikaka7891、kaxika7891或者7891akakxi，表面看上去是没有规律的。
- 使用一句话来设置密码。例如“好好学习，天天向上”，一般都会想到分别取每个字的第一个字母，即hhxxttxs，在设置时可结合前面介绍的技巧来设置，如HhxxTtxs,H2x2t2xs。
- 注意在电脑中安装比较可靠的杀毒软件。如果用户的电脑中含有木马，那么再复杂的密码也是没有任何作用的。
- 定期更改密码。长时间使用相同的密码也很容易被识破，因此建议用户每个月或者每几个月就重新设置密码。
- 不要在所有的地方都使用同一个密码。用户可根据重要性的原则来设定密码，一般不是非常重要的地方可设置相对简单的密码。
- 不要把密码写在别人能够看得见的地方，有些用户为了防止忘记密码常常将密码用笔记录下来，例如笔记本、纸巾上等，这些地方很容易被其他人看见。其实最好的方法就是强制性的记忆在脑子里，在输入密码时不要让别人看见，反复在键盘上练习几次，更不要把密码告诉别人。

Chapter 03

系统安全设置

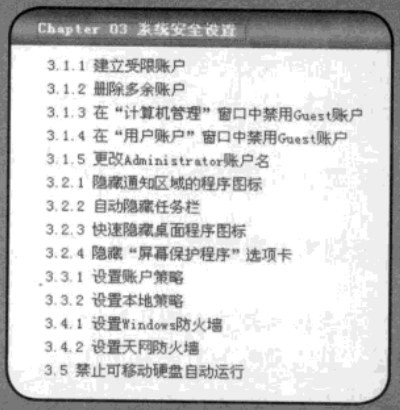
重点知识

1. 系统账户设置
2. 桌面设置
3. 系统安全策略
4. 使用防火墙

为了确保电脑安全，除可以为电脑设置密码外，还可以在电脑中新建账户和更改Administrator名称以扰乱其他人对计算机管理员账户的判断，也可以在桌面上隐藏一些重要的信息，如隐藏桌面上的快捷图标。另外还需要使用防火墙，可以设置操作系统自带的Windows防火墙，也可以使用比较出名的天网防火墙。

视频文件

参见随书光盘：视频教程\Chapter 03



3.1 系统账户设置

用户账户是用来记录用户的用户名、口令、个人文件和设置等信息。在安装操作系统的过程中需要创建新账户。为了保障账户安全，可在电脑中执行建立受限账户、禁用Guest账户和更改Administrator账户名等操作，使电脑中携带有重要数据的账户或管理员账户更加安全。同时，为了节约系统资源，用户也可删除一些不常用的账户。

3.1.1 建立受限账户

用户进入操作系统后若想创建新的账户有两种选择，即创建计算机管理员账户和受限账户，为了安全，建议用户建立受限账户。

① 单击“控制面板”命令

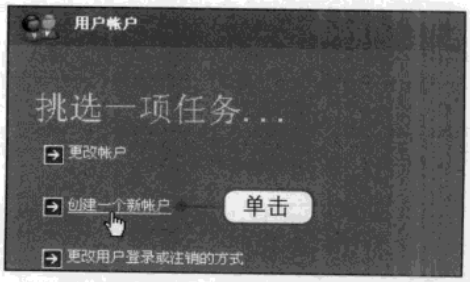
①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“控制面板”命令。

② 双击“用户账户”图标

打开“控制面板”窗口，在窗口中双击“用户账户”图标。

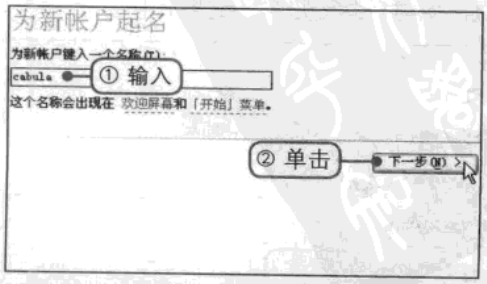
③ 创建一个新账户

打开“用户账户”窗口，在“挑选一项任务”选项组中单击“创建一个新账户”文字链接。



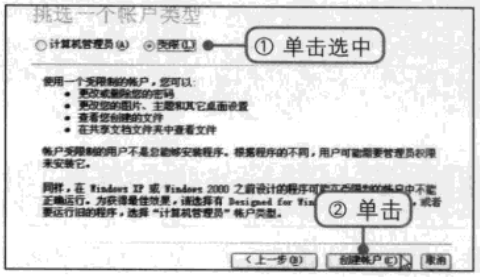
④ 输入新账户名

打开“为新账户起名”界面，①在“为新账户键入一个名称”文本框中输入新账户的名称。②单击“下一步”按钮。



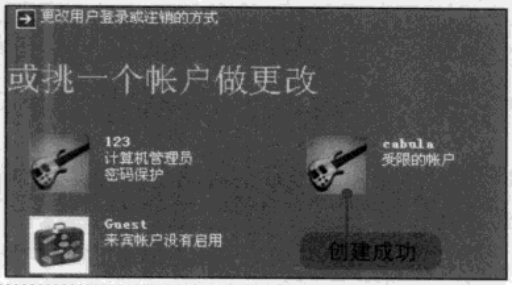
⑤ 选择账户类型

打开“挑选一个账户类型”界面，①单击选中“受限”单选按钮。②单击“创建账户”按钮。



⑥ 创建成功

返回“用户账户”主界面窗口，此时可在“或挑一个账户做更改”选项组中看见新创建的受限账户。



3.1.2 删除多余账户

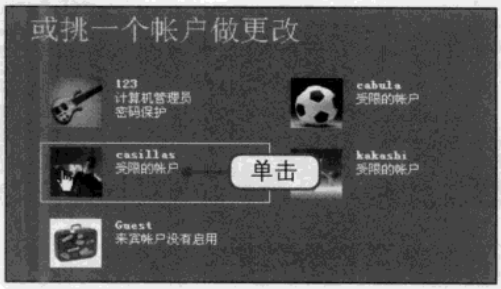
当电脑中的账户太多时，可以删除一些不常用的账户以节约系统资源。具体操作如下。

① 打开“用户账户”窗口

按照前面介绍的方法打开“控制面板”窗口，在窗口中双击“用户账户”图标，打开“用户账户”窗口。

② 选中需要删除的账户

在“或挑一个账户做更改”选项组中单击需要删除的账户。

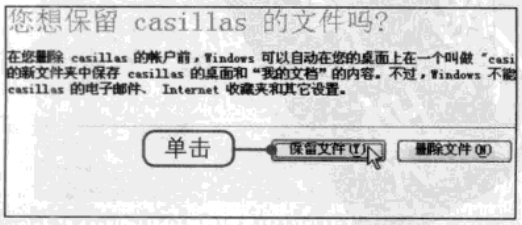


③ 删除账户

打开“您想更改casillas的账户的什么？”界面，单击“删除账户”文字链接。

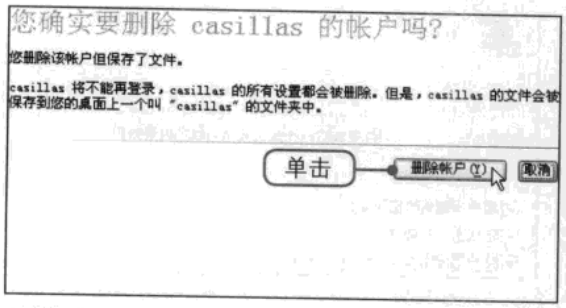
④ 保留文件

切换至“您想保留casillas的文件吗？”界面，用户可自行选择是否保留文件，例如单击“保留文件”按钮。



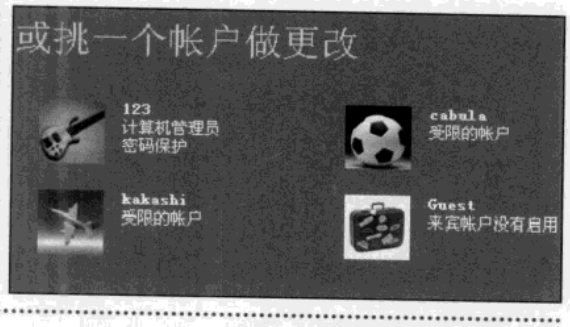
⑤ 确认删除账户

打开“您确实要删除casillas的账户吗？”界面，确认无误后单击“删除账户”按钮。



⑥ 删除成功

返回“用户账户”主界面窗口，此时可在窗口中看见casillas账户已经被删除。

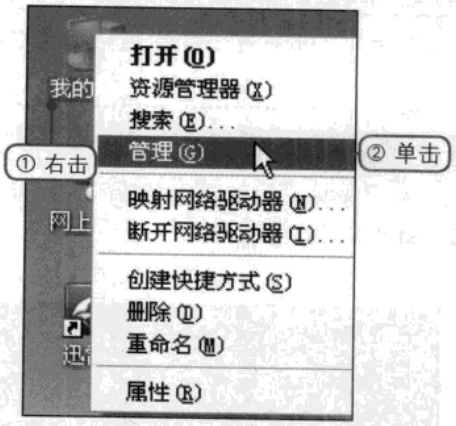


3.1.3 在“计算机管理”窗口中禁用Guest账户

Guest账户即所谓的来宾账户，使用该账户可以访问电脑，但是没有管理员账户的权限大。用户可通过禁用Guest账户来防止黑客通过该账户入侵电脑。右击“我的电脑”图标，接着在弹出的快捷菜单中单击“管理”命令，打开“计算机管理”窗口，然后就可禁用Guest账户。

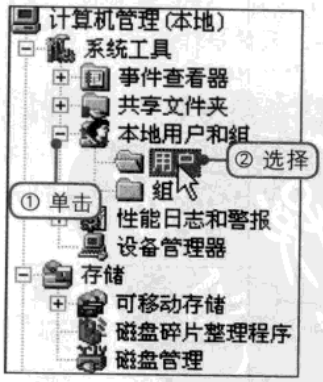
① 单击“管理”命令

①右击“我的电脑”图标。②在弹出的快捷菜单中单击“管理”命令。



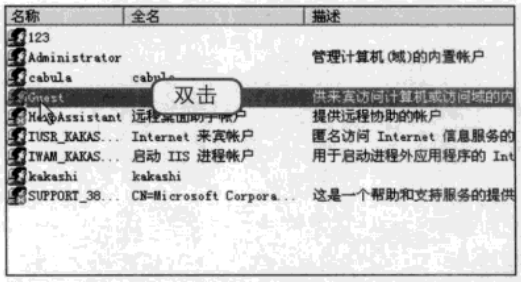
② 选择“用户”选项

打开“计算机管理”窗口，①单击窗口左侧的“本地用户和组”前的展开按钮。②选择“用户”选项。



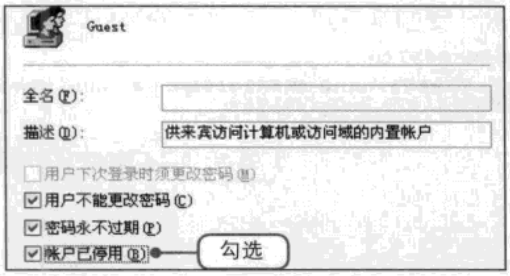
③ 双击Guest选项

在“计算机管理”窗口的右侧双击Guest选项，打开“Guest属性”对话框。



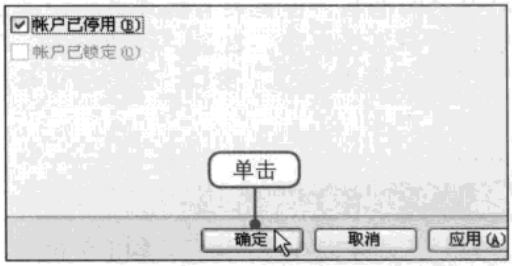
④ 禁用Guest账户

在窗口中勾选“账户已停用”复选框，即禁用Guest账户。



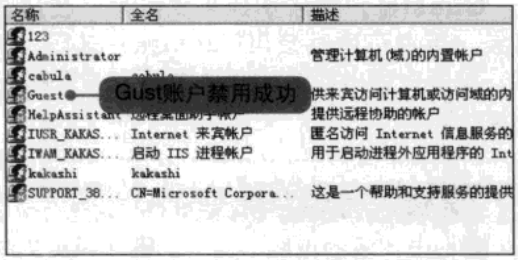
⑤ 单击“确定”按钮

单击窗口下方的“确定”按钮，返回“计算机管理”窗口。



⑥ 禁用成功

此时可看见Guest图标下方有一个红色符号，即禁用成功。



3.1.4 在“用户账户”窗口中禁用Guest账户

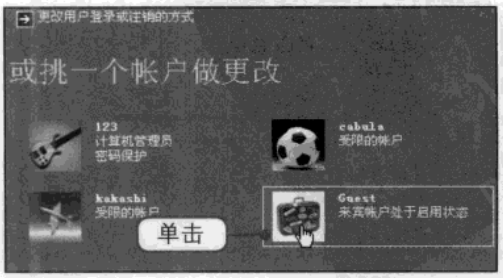
除了可以在“计算机管理”窗口中禁用Guest账户之外，也可在“用户账户”窗口中禁用Guest账户。具体操作如下。

① 打开“用户账户”窗口

按照前面介绍的方法打开“控制面板”窗口，双击“用户账户”图标，打开“用户账户”窗口。

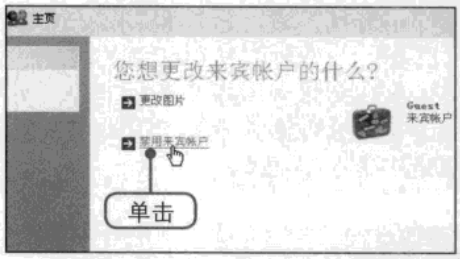
② 单击Guest账户

在“或挑一个账户做更改”选项组中单击Guest账户对应的图标。



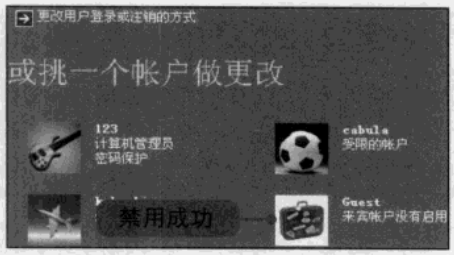
③ 禁用来宾账户

打开“您想更改来宾账户的什么”界面，单击“禁用来宾账户”文字链接。



④ 禁用成功

返回“用户账户”窗口，此时可看见“来宾账户没有启用”字样，成功禁用Guest账户。

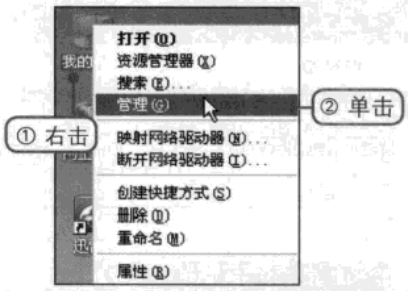


3.1.5 更改Administrator账户名

当在电脑中安装Windows XP操作系统后，系统会自动创建一个Administrator账户，用户可尝试更改该账户的账户名以防止他人以管理员的身份进入电脑。

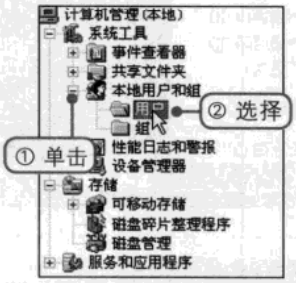
① 单击“管理”命令

①右击“我的电脑”图标。②在弹出的快捷菜单中单击“管理”命令。



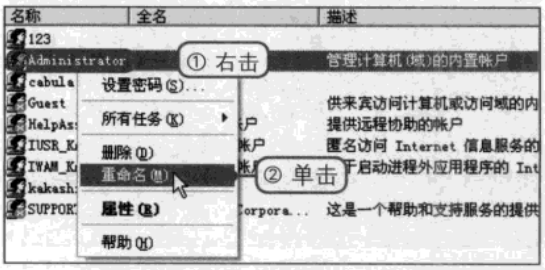
② 选择“用户”选项

打开“计算机管理”窗口，①单击窗口左侧的“本地用户和组”前的展开按钮。②选择“用户”选项。



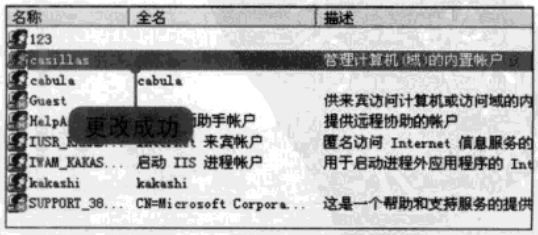
③ 单击“重命名”命令

①右击窗口右侧的Administrator选项。②在弹出的快捷菜单中单击“重命名”命令。



④ 更改成功

此时Administrator选项处于可编写状态，输入新的账户名并按Enter键，用户可以看见该账户已经成功更改。



3.2 桌面设置

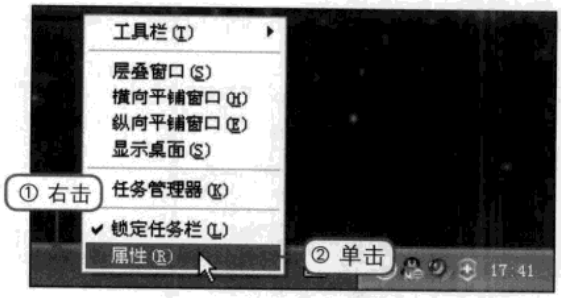
桌面是打开计算机并登录到Windows之后看到的主屏幕区域，它就像实际的桌面一样，是用户工作的平台。Windows桌面主要由桌面图标、“开始”按钮和任务栏三部分组成。用户还可以将一些项目（如文件或者文件夹）放在桌面上，并且随意排列。用户所打开的程序或者文件夹也会显示在桌面上。因此对桌面进行相关设置对保护电脑重要信息的安全也十分重要，如隐藏桌面图标、隐藏通知区域的程序图标等。

3.2.1 隐藏通知区域的程序图标

通知区位于任务栏的最右边，包括时钟、音量控制状态等其他图标，当系统安装了软件和驱动程序并成功设置为开机后软件自动加载时，则开机后通知区域就会出现加载项。用户可在通知区域中隐藏一些重要的应用程序图标。

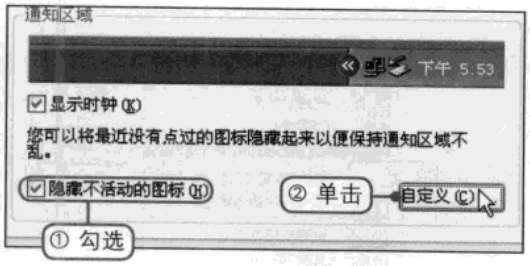
① 单击“属性”命令

①右击任务栏中的任意空白处。②在弹出的快捷菜单中单击“属性”命令。



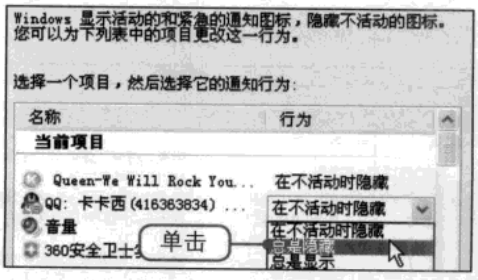
② 单击“自定义”按钮

打开“任务栏和「开始」菜单属性”对话框，①勾选“隐藏不活动的图标”复选框。②单击“自定义”按钮。



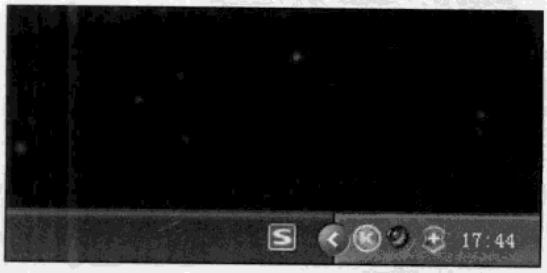
③ 设置为总是隐藏

打开“自定义通知”对话框，选中需要隐藏的项目，在右侧对应的下拉列表框中选择“总是隐藏”选项。



④ 设置成功

返回桌面，此时用户会在状态栏的“通知区域”中看见设置的项目已经隐藏。

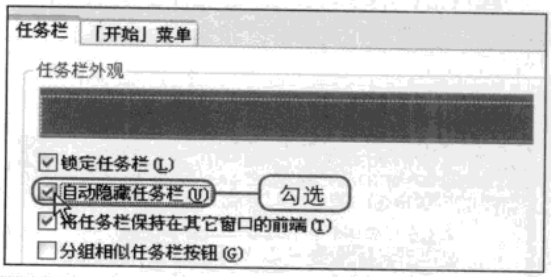


3.2.2 自动隐藏任务栏

如果要隐藏通知区域中的重要图标，但是通知区域仍然保留在状态栏中，这时可通过设置将任务栏自动隐藏。

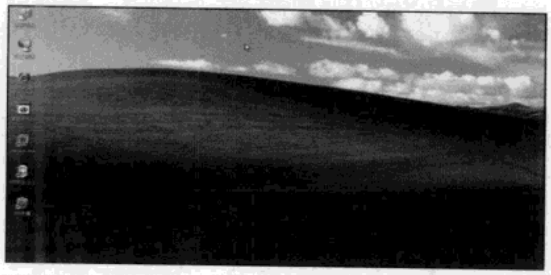
① 勾选“自动隐藏任务栏”复选框

按照前面的方法打开“任务栏和「开始」菜单属性”对话框，勾选“自动隐藏任务栏”复选框。



② 设置成功

单击“确定”按钮返回桌面，此时可看见状态栏已经自动被隐藏。

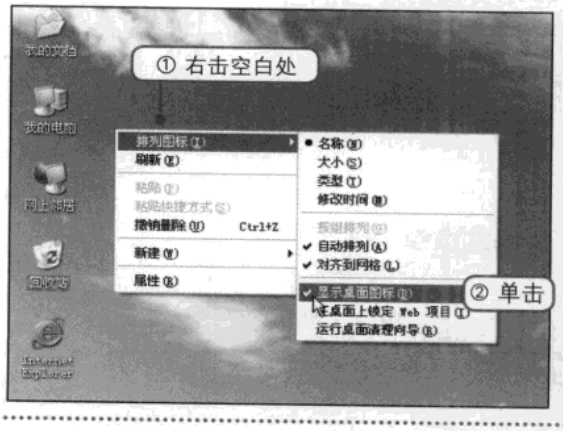


3.2.3 快速隐藏桌面程序图标

桌面上除了任务栏之外，还有“开始”菜单和桌面图标。如果设置了自动隐藏任务栏，则“开始”按钮也随着被隐藏。用户要是觉得桌面还不够安全，则可以快速隐藏桌面上的所有图标。

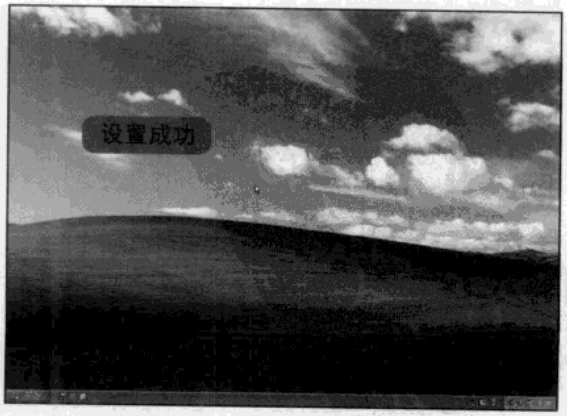
① 取消勾选“显示桌面图标”命令

①右击桌面上的任意空白处。②在弹出的快捷菜单中单击“排列图标”命令并取消勾选其级联菜单中的“显示桌面图标”命令。



② 设置成功

返回桌面，此时可以看见桌面上的程序图标全部消失，则设置成功。若要显示这些图标，勾选“显示桌面图标”命令即可。



3.2.4 隐藏“屏幕保护程序”选项卡

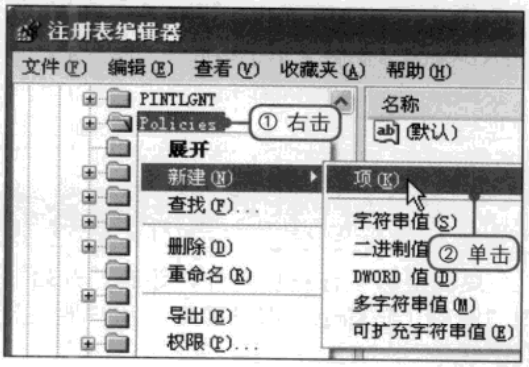
当液晶显示器电脑或者笔记本电脑使用屏幕保护程序时，其显示器中的液晶分子是一直处于开关工作状态的，而液晶分子的开关次数会受到寿命的限制。因此，使用屏幕保护程序会使显示器的寿命减少，并且在使用一段时间后会在显示器上出现坏点。用户可在注册表中通过设置来隐藏“显示 属性”对话框中的“屏幕保护程序”选项卡。

① 查找Policies选项

按照2.5.1小节所述的方法打开“注册表编辑器”窗口，在HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion文件夹下找到Policies选项。

② 新建子项

①右击Policies选项。②在弹出的快捷菜单中单击“新建>项”命令，新建一个子项。

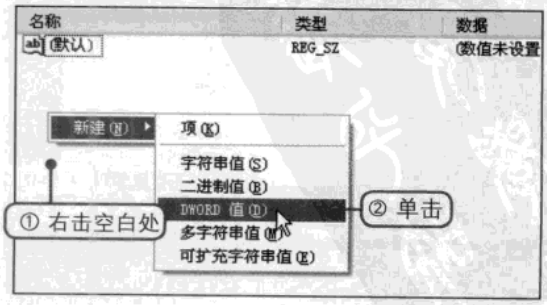


③ 命名为system

此时新建的子项名处于可编写状态，将其命名为system并按Enter键。即system子项创建成功。

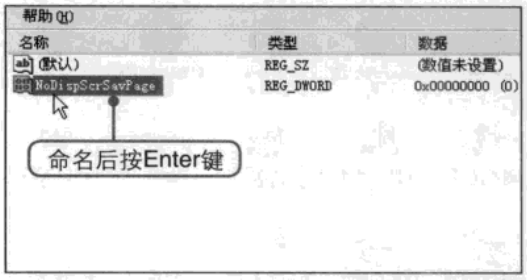
④ 新建DWORD值

选中system子项，①右击窗口右侧的任意空白处。②在弹出的快捷菜单中单击“新建>DWORD值”命令。



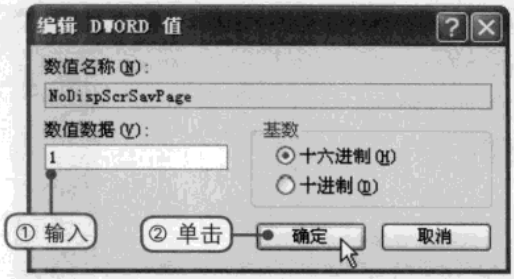
⑤ 命名为NoDispScrSavPage

此时新建的DWORD值名处于可编写状态，将其命名为NoDispScrSavPage并按Enter键。



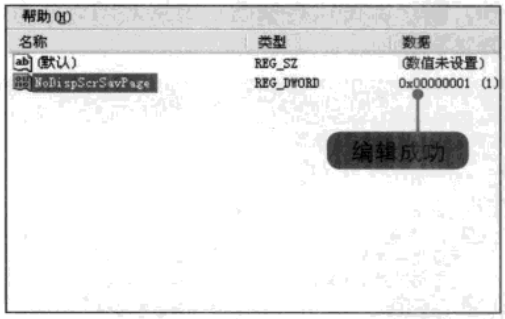
⑥ 编辑DWORD值

双击NoDispScrSavPage选项，弹出“编辑DWORD值”对话框，①在“数值数据”文本框中输入1。②单击“确定”按钮。



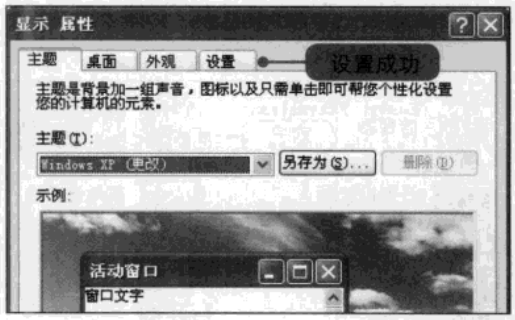
⑦ 编辑成功

返回“注册表编辑器”窗口，此时可在窗口的右侧看见NoDispScrSavPage选项的数据值为1，关闭窗口返回桌面。



⑧ 查看“显示 属性”对话框

打开“显示 属性”对话框，此时可以在该对话框中看见“屏幕保护程序”选项卡已经被隐藏了。



3.3 设置本地安全策略

Windows XP操作系统自带的“本地安全策略”是一个很不错的系统安全管理工具，用户可通过它对计算机安全和权限进行设置。“本地安全策略”管理工具可用来直接修改本地计算机的账户策略和本地策略等选项的设置。

3.3.1 设置账户策略

账户策略包括密码策略和账户锁定策略，密码策略主要是对密码必须符合复杂性要求、密码长度最小值和密码的存留期进行相关设置；而账户锁定策略则是对账户锁定阈值、账户锁定时间和复位账户锁定计数器进行设置。

① 打开“控制面板”窗口

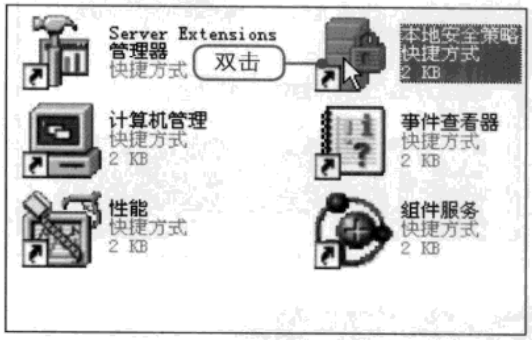
①单击桌面上的“开始”按钮，②在弹出的“开始”菜单中单击“控制面板”命令，打开“控制面板”窗口。

② 打开“管理工具”窗口

在“控制面板”窗口中双击“管理工具”图标，打开“管理工具”窗口。

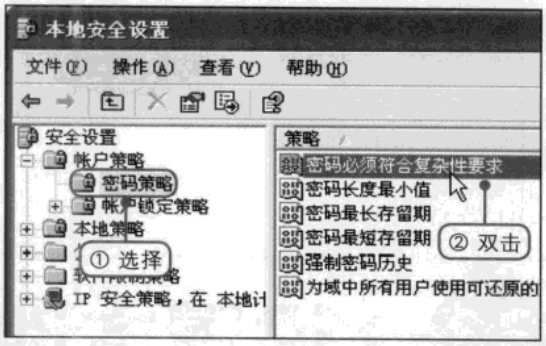
③ 打开“本地安全策略”窗口

在“管理工具”窗口中双击“本地安全策略”图标，打开“本地安全设置”窗口。



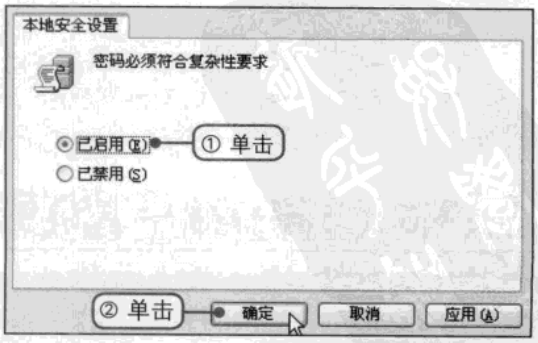
④ 设置密码必须符合复杂性要求

①在窗口左侧选择“账户策略>密码策略”选项。②双击窗口右侧的“密码必须符合复杂性要求”选项。



⑤ 启用密码必须符合复杂性要求

弹出“密码必须符合复杂性要求属性”对话框，①单击选中“已启用”单选按钮。②然后单击“确定”按钮。



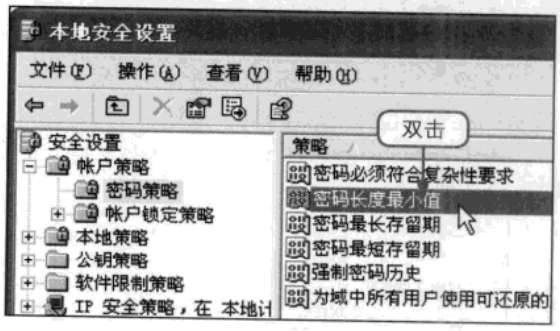
密码复杂性要求

用户启用密码必须符合复杂性要求时，所设置的密码必须满足以下最低要求。

- 不包含全部或部分的用户账户名。
- 长度至少为6个字符。
- 密码要包含来自英文大写字母（从A到Z）、英文小写字母（从a到z）、10个基本数字（从0到9）和非字母字符4个类别中的3个字符。

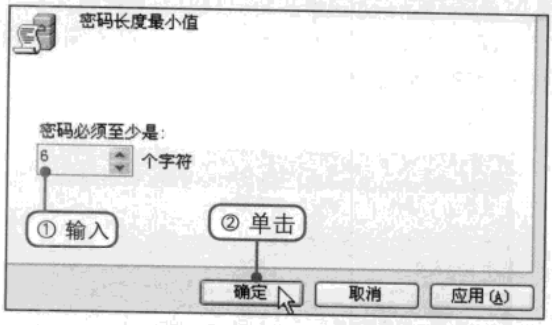
⑥ 双击“密码长度最小值”选项

返回“本地安全设置”窗口，双击窗口右侧的“密码长度最小值”选项，打开“密码长度最小值属性”对话框。



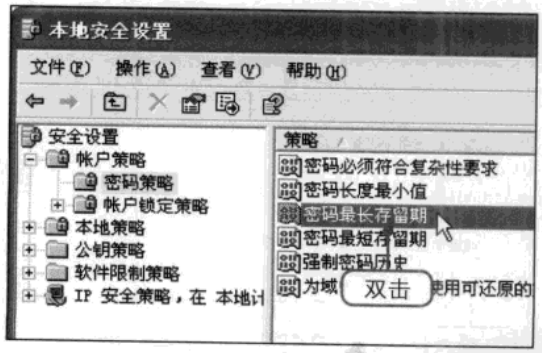
⑦ 设置密码长度最小值

①在“密码必须至少是”微调框中输入密码长度最小值，如输入6。②单击“确定”按钮。



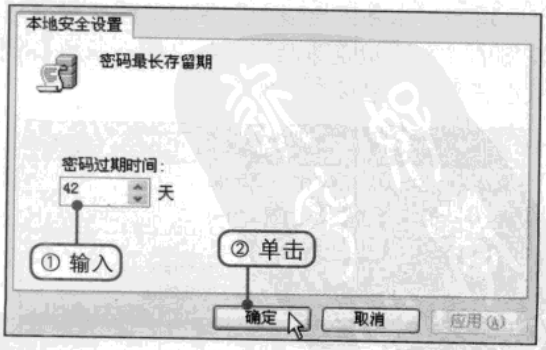
⑧ 双击“密码最长存留期”选项

返回“本地安全设置”窗口，双击窗口右侧的“密码最长存留期”选项。



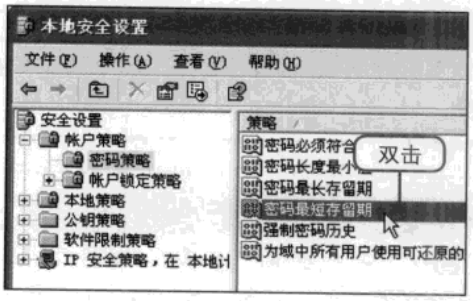
⑨ 设置密码最长存留期

弹出“密码最长存留期属性”对话框，①在“密码过期时间”微调框中输入密码过期的时间。②单击“确定”按钮。



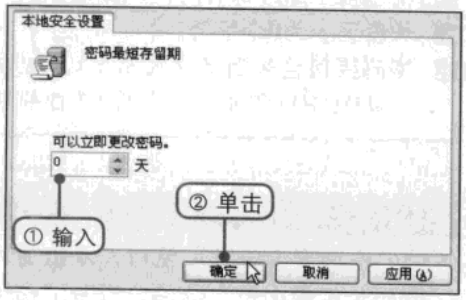
10 双击“密码最短存留期”选项

返回“本地安全设置”窗口，双击窗口右侧的“密码最短存留期”选项。



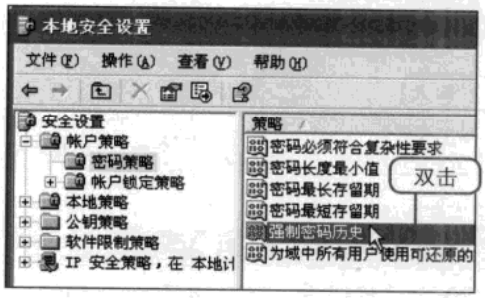
11 设置密码最短存留期

弹出“密码最短存留期属性”对话框，①在“可以立即更改密码”微调框中输入0，表示可以立即更改密码。②单击“确定”按钮。



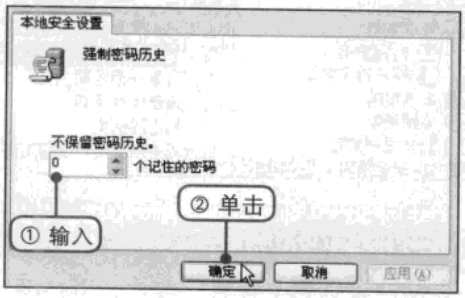
12 双击“强制密码历史”选项

返回“本地安全设置”窗口，双击窗口右侧的“强制密码历史”选项。



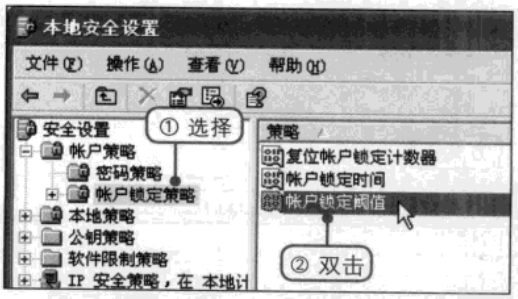
13 设置强制密码历史

弹出“强制密码历史属性”对话框，①在“不保留密码历史”微调框中输入0，表示不保留密码历史。②单击“确定”按钮。



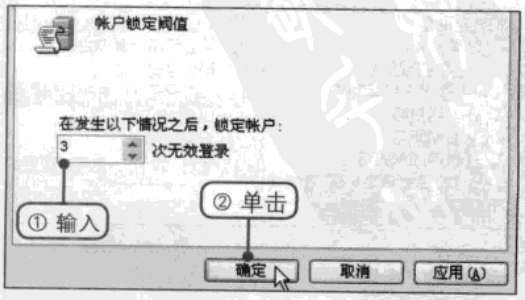
14 双击“账户锁定阈值”选项

返回“本地安全设置”窗口，①选择窗口左侧的“账户锁定策略”选项。②在窗口右侧双击“账户锁定阈值”选项。



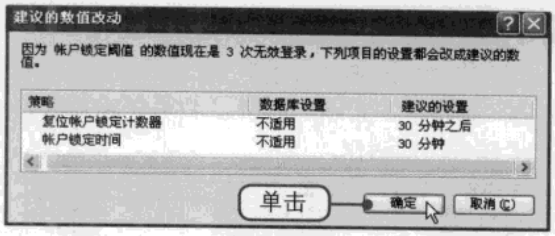
15 设置账户锁定阈值

弹出“账户锁定阈值属性”对话框，①在“在发生以下情况之后，锁定账户”微调框中输入数值，设置无效登录的次数。②单击“确定”按钮。



⑯ 确认建议的数值改动

弹出“建议的数值改动”对话框，用户可保持系统建议的数值改动，也可手动设置其他两个选项，单击“确定”按钮。



账户锁定阈值

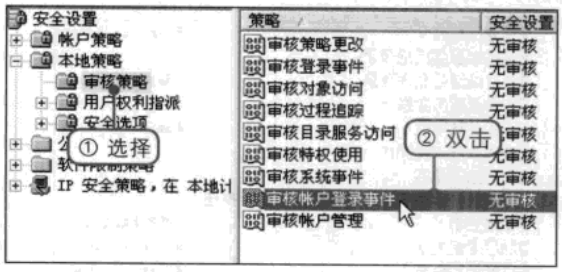
账户锁定阈值是用来确定尝试登录失败多少次后锁定用户账户。锁定后，只有在管理员账户进行重新设置或者锁定期已满的情况下才可再次使用锁定的账户。账户锁定阈值可设置为1～999之间的值，若设置为0则表示系统始终不锁定该账户。对于使用Ctrl+Alt+Delete组合键或带有密码保护的屏幕保护程序锁定的工作站或电脑上，失败的密码尝试不计入失败的登录尝试次数。

3.3.2 设置本地策略

本地策略包括审核策略、用户权利指派和安全选项三方面。审核策略是确定是否将安全事件记录到电脑上的安全日志中；用户权利指派是确定哪些用户或组具有登录电脑的权利或者特权；安全选项是启用或禁用电脑的安全设置。

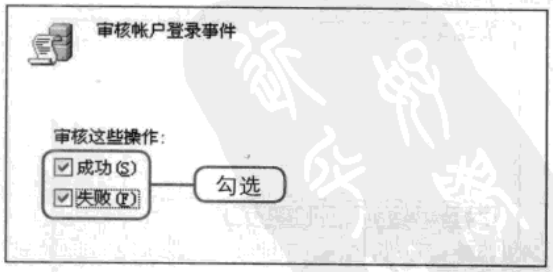
① 双击“审核账户登录事件”选项

打开“本地安全设置”窗口，①在窗口左侧选择“本地策略>审核策略”选项。②双击窗口右侧的“审核账户登录事件”选项。



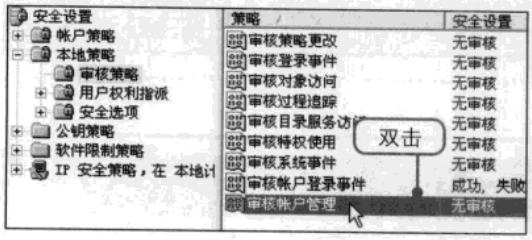
② 设置审核账户登录事件

弹出“审核账户登录事件 属性”对话框，勾选“成功”和“失败”复选框。然后单击“确定”按钮。



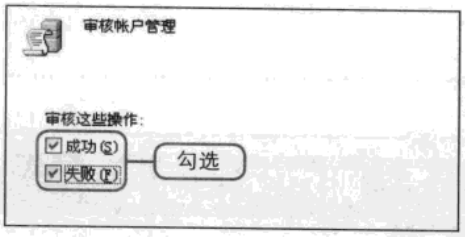
③ 双击“审核账户管理”选项

返回“本地安全设置”窗口，双击窗口右侧的“审核账户管理”选项，打开“审核账户管理 属性”对话框。



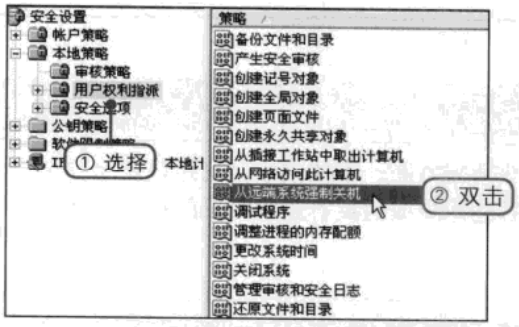
④ 设置审核账户管理

在“审核账户管理 属性”对话框中勾选“成功”和“失败”复选框。然后单击“确定”按钮。



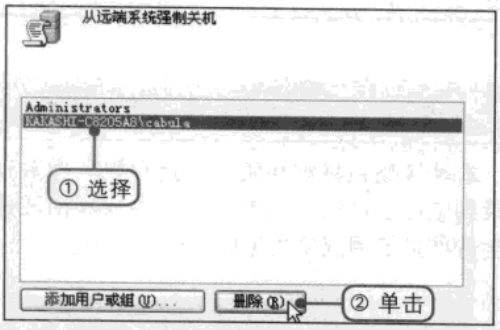
⑤ 双击“从远端系统强制关机”选项

返回“本地安全设置”窗口，①在窗口左侧选择“用户权利指派”选项。②双击窗口右侧的“从远端系统强制关机”选项。



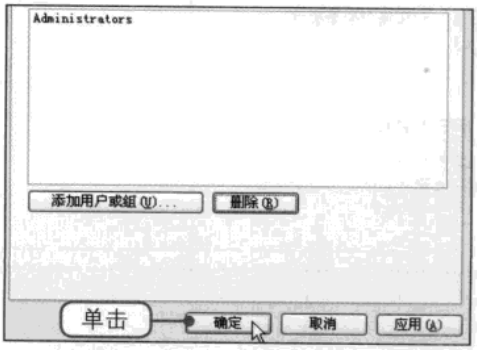
⑥ 删除多余的用户

弹出“从远端系统强制关机 属性”对话框，①在列表框中选择需要删除的用户。②单击“删除”按钮。



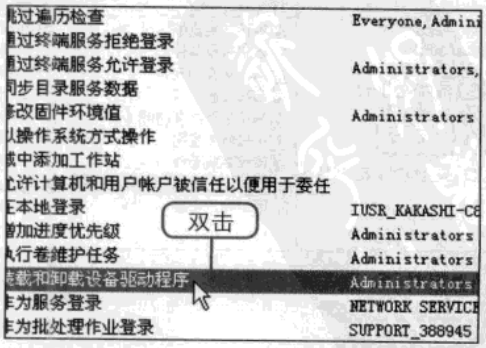
⑦ 成功删除

此时可在对话框中看见选中的用户已经被删除，直接单击“确定”按钮。



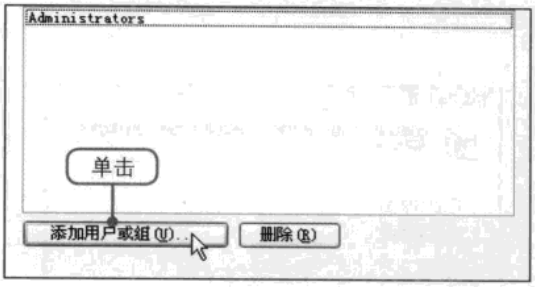
⑧ 双击“装载和卸载设备驱动程序”选项

返回“本地安全设置”窗口，双击窗口右侧的“装载和卸载设备驱动程序”选项。



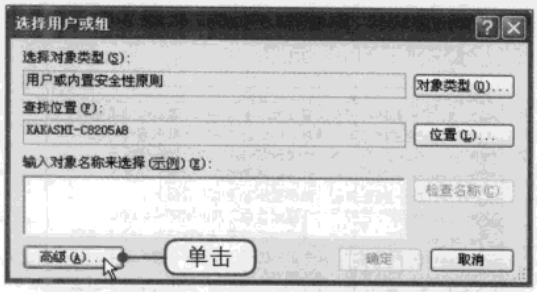
⑨ 设置装载和卸载设备驱动程序

打开“装载和卸载设备驱动程序 属性”对话框，单击“添加用户或组”按钮。



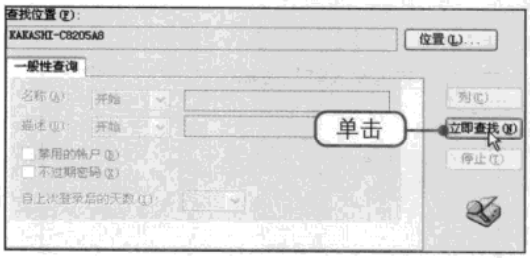
⑩ 单击“高级”按钮

弹出“选择用户或组”对话框，单击“高级”按钮。



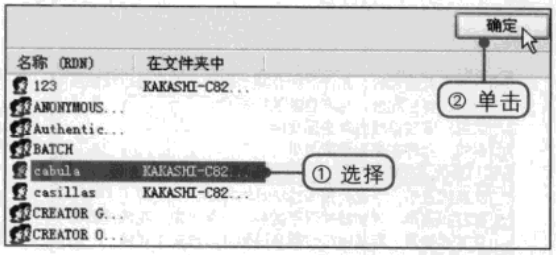
⑪ 单击“立即查找”按钮

在“选择用户或组”对话框中部显示了“一般性查询”选项卡，单击“立即查找”按钮。



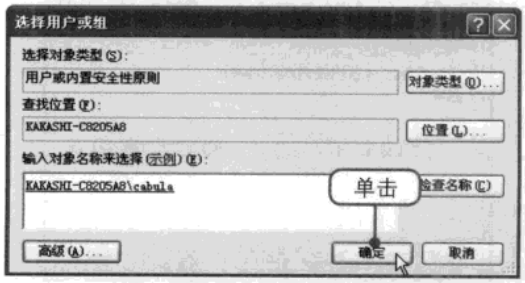
⑫ 选中添加的用户

①在“选择用户或组”对话框下方的列表框中选择需要添加的用户。②单击“确定”按钮。



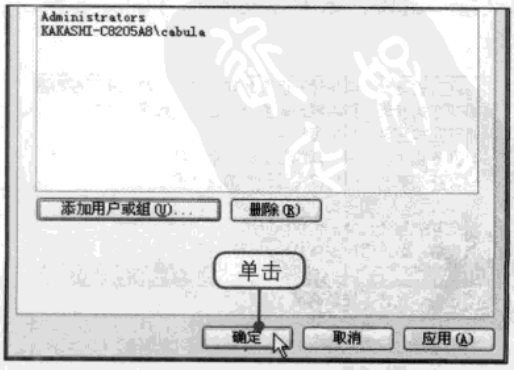
⑬ 单击“确定”按钮

由于选中的用户并不是手动输入的，无需检查名称。直接单击“确定”按钮返回“装载和卸载设备驱动程序”对话框。



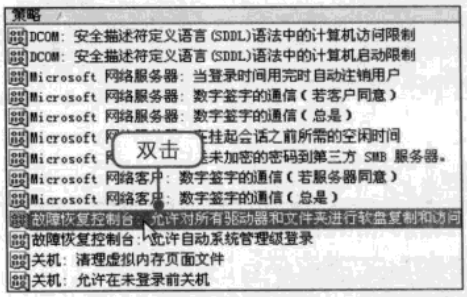
⑭ 成功添加

此时可在“装载和卸载设备驱动程序”对话框中看见添加的用户，单击“确定”按钮完成添加。



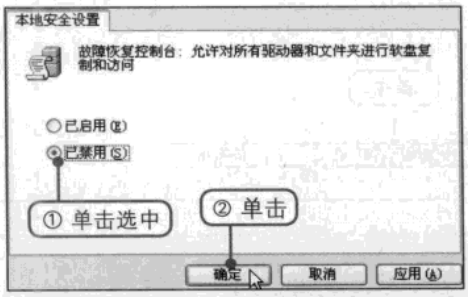
15 设置故障恢复控制台

返回“本地安全设置”窗口，选择窗口左侧的“安全选项”选项，在窗口右侧双击“故障恢复控制台：允许对所有驱动器和文件夹进行软盘复制和访问”选项。



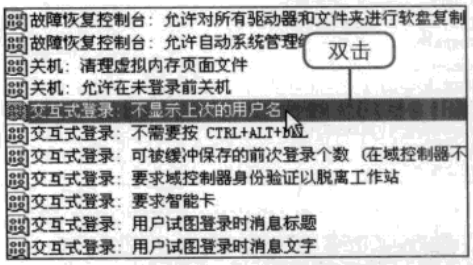
16 禁用该选项

①在弹出的对话框中单击选中“已禁用”单选按钮。②单击“确定”按钮。



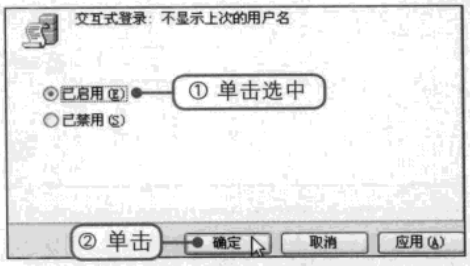
17 双击“不显示上次的用户名”选项

返回“本地安全设置”窗口，在窗口的右侧双击“交互式登录：不显示上次的用户名”选项。



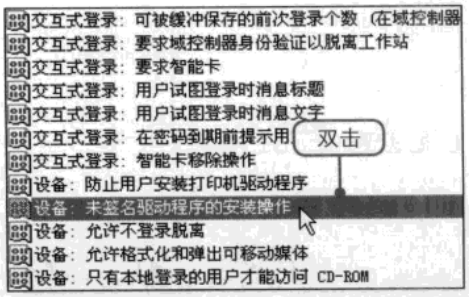
18 启用不显示上次的用户名

弹出“交互式登录：不显示上次的用户名属性”对话框，①单击选中“已启用”单选按钮。②单击“确定”按钮。



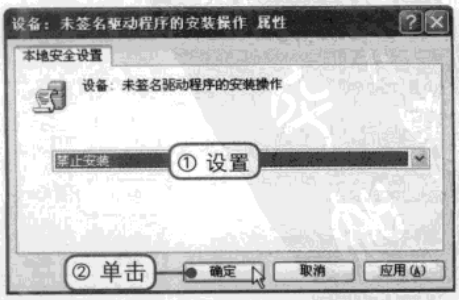
19 未签名驱动程序的安装操作

返回“本地安全设置”窗口，在窗口的右侧双击“设备：未签名驱动程序的安装操作”选项 。



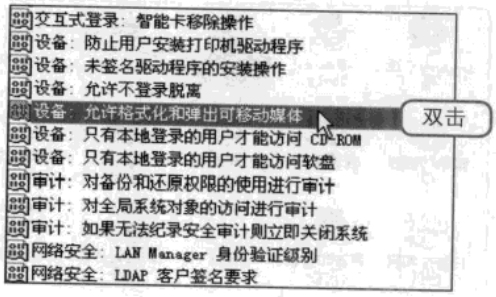
20 选择“禁止安装”选项

弹出“设备：未签名驱动程序的安装操作属性”对话框，①设置为禁止安装未签名的驱动程序。②单击“确定”按钮。



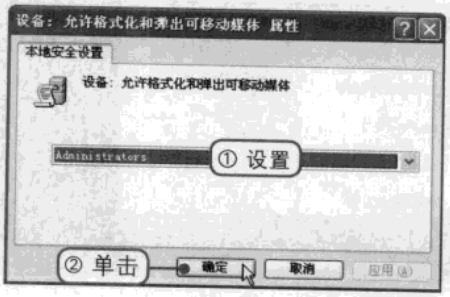
21 允许格式化和弹出可移动媒体

返回“本地安全设置”窗口，在窗口右侧双击“设备：允许格式化和弹出可移动媒体”选项。



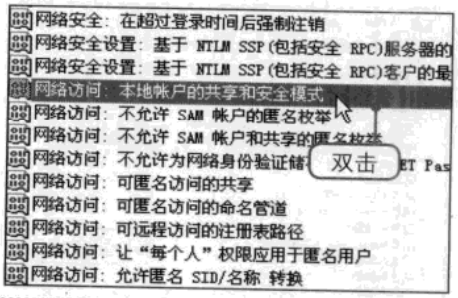
22 选择Administrator选项

弹出“设备：允许格式化和弹出可移动媒体 属性”对话框，①设置为只有Administrator可以进行该操作。②单击“确定”按钮。



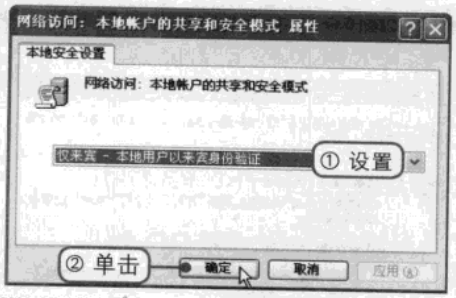
23 本地账户的共享和安全模式

返回“本地安全设置”窗口，在窗口右侧双击“网络访问：本地账户的共享和安全模式”选项。



24 选中“仅来宾”选项

弹出“网络访问：本地账户的共享和安全模式 属性”对话框，①设置为仅来宾－本地用户以来宾身份验证。②单击“确定”按钮。



3.4 使用防火墙

防火墙是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，是一个位于电脑和它所连接的网络之间的硬件或者软件。电脑中流入流出的所有网络通信均要经过防火墙，它能阻隔因特网上破坏者的入侵，有助于提高电脑的安全性。

3.4.1 设置Windows防火墙

Windows防火墙将限制从其他电脑发送到用户电脑的信息，这使得用户自己可以更好的控制电脑中的数据，并针对一些未经邀请而尝试连接到用户电脑的其他用户或者程序提供了一条防御线。防火墙检查来自网络的信息，然后根据防火墙的设置拒绝或允许信息的到达。

① 打开“控制面板”窗口

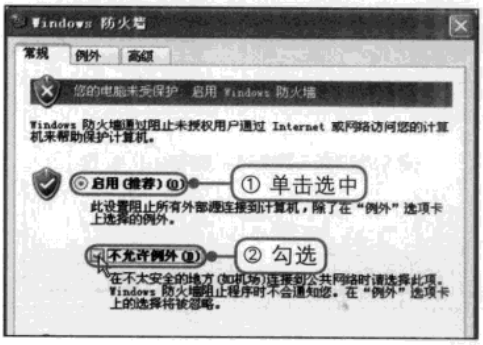
①单击桌面上的“开始”按钮，②在弹出的“开始”菜单中单击“控制面板”命令，打开“控制面板”窗口。

② 打开“Windows防火墙”对话框

在“控制面板”窗口中双击“Windows防火墙”图标，打开“Windows防火墙”对话框。

③ 启用Windows防火墙

①在“Windows防火墙”对话框中单击选中“启用”按钮。②在下方勾选“不允许例外”复选框。

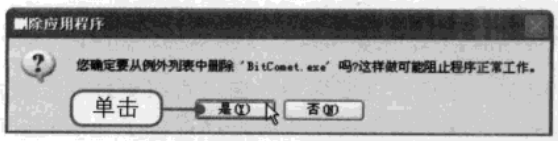


④ 删除不需要的程序和服务

①单击“例外”标签切换至“例外”选项卡。②在“程序和服务”列表框中勾选不需要的程序和服务。③单击“删除”按钮。

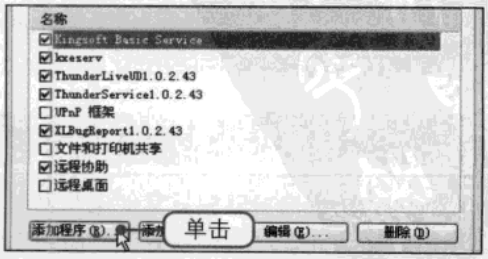
⑤ 确定删除

弹出“删除应用程序”对话框，用户确认选择的程序和服务无误后单击“是”按钮。



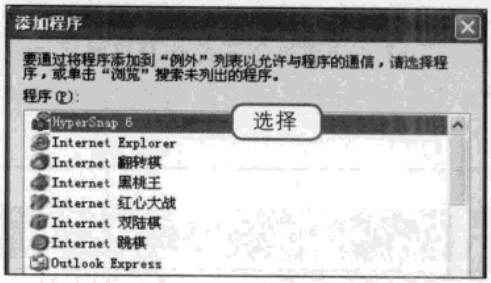
⑥ 添加程序

返回“Windows防火墙”对话框的“例外”选项卡，可单击“添加程序”按钮添加程序和服务。



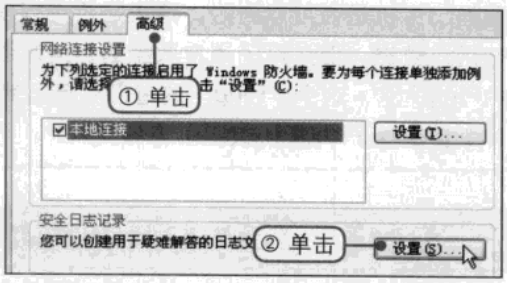
⑦ 选择添加的程序

弹出“添加程序”对话框，在“程序”列表框中选择需要添加的程序，然后单击“确定”按钮。



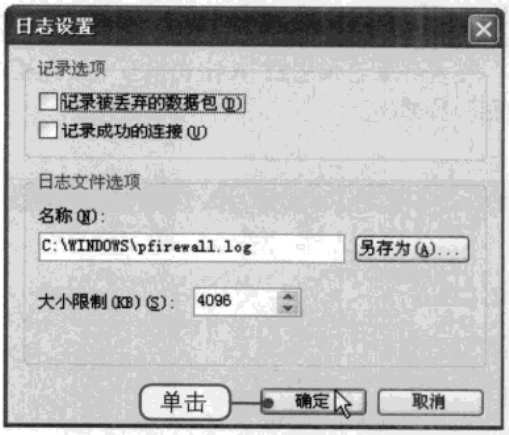
⑧ 单击“设置”按钮

返回“Windows防火墙”对话框，①单击“高级”标签切换至该选项卡。②在“安全日志记录”选项组中单击“设置”按钮。



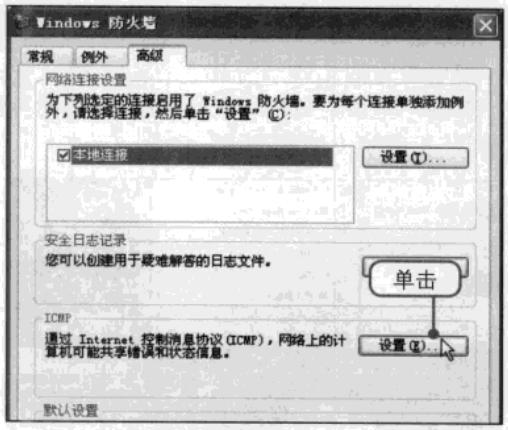
⑨ 日志设置

弹出“日志设置”对话框，用户可根据自身的需要对记录选项、日志文件选项进行设置，设置完成后，单击“确定”按钮。



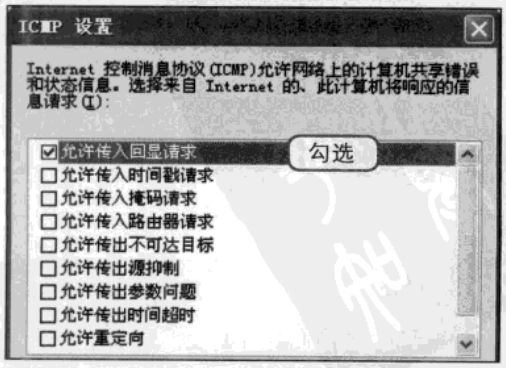
⑩ 单击“设置”按钮

返回“Windows防火墙”对话框，在“高级”选项卡下单击ICMP选项组中的“设置”按钮。



⑪ ICMP设置

弹出“ICMP设置”对话框，用户可根据自身的需要对其进行设置，设置完成后单击“确定”按钮即可。



新手学堂

ICMP的作用

ICMP（Internet Control Message Protocol，Internet控制报文协议）是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络是否通畅、主机是否可以到达、路由是否可以使用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。经常使用的用于检查网络是否通畅的Ping命令，这个“Ping”的过程实际上就是ICMP协议工作的过程；还有跟踪路由的Tracert命令也是基于ICMP协议。

3.4.2 设置天网防火墙

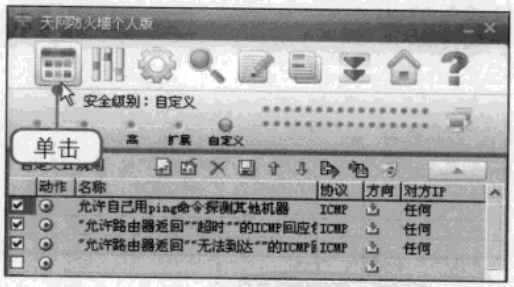
天网防火墙是为个人电脑提供的网络安全程序工具，它根据管理者设定的安全规则把守网络，为用户保护重要信息。天网防火墙还提供强大的访问控制、信息过滤等功能，让用户能安全的上网。在使用天网防火墙之前需首先启用该软件，而安装该软件后在桌面上没有对应的快捷图标，但可通过“开始”菜单启用该软件，启用后可对应用程序规则、系统设置等选项按照自身的需求进行设置。

① 启用天网防火墙

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“所有程序>天网防火墙试用版>天网防火墙试用版”命令。

② 单击“应用程序规则”按钮

在主界面下单击 按钮切换至“应用程序规则”界面下。

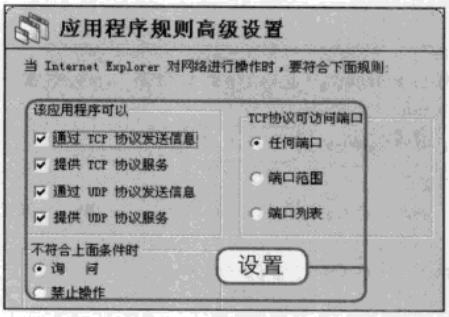


③ 选中需设置的应用程序

在下方的列表框中选择需要设置的应用程序，例如选择Internet Explorer选项，单击该选项右侧的“选项”按钮。

4 设置应用程序规则

弹出“应用程序规则高级设置”对话框，在该对话框中用户可根据自身条件进行设置。设置完成之后单击“确定”按钮。

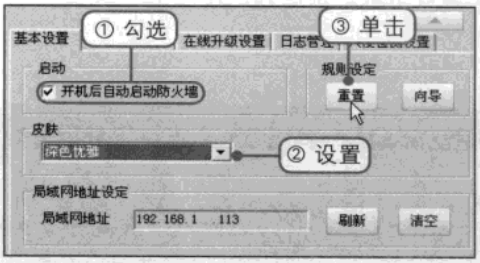


5 单击“系统设置”按钮

返回该软件主界面，单击顶部的按钮切换至“系统设置”界面下。

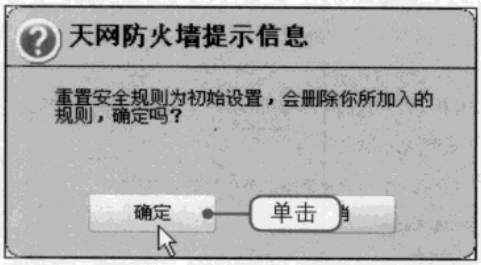
6 基本设置

①在“基本设置”选项卡勾选 “开机后自动启动防火墙”复选框。②设置皮肤为“深色优雅”。③单击“重置”按钮。



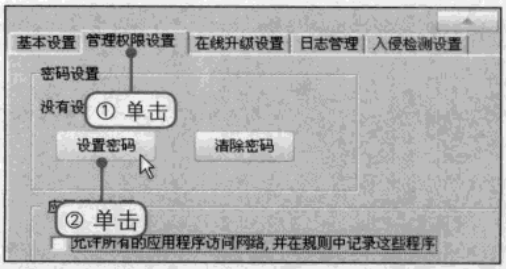
7 确认重置

此时弹出“天网防火墙提示信息”提示框，确认是否重置安全规则为初始设置，然后单击“确定”按钮。



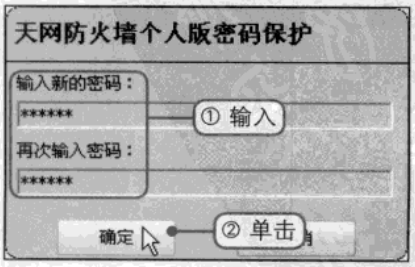
8 单击“设置密码”按钮

①单击“管理权限设置”标签切换至该选项卡。②单击“设置密码”按钮。



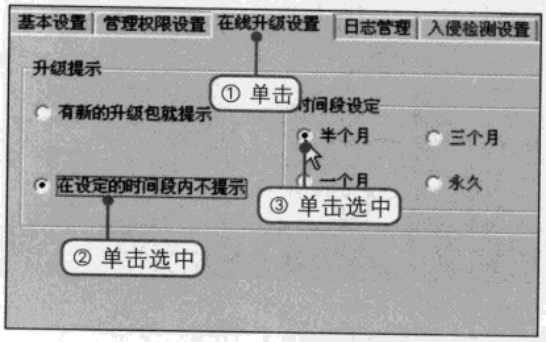
9 设置密码

弹出“天网防火墙个人版密码保护”对话框，①在文本框中设置密码。②设置完成之后单击下方的“确定”按钮。



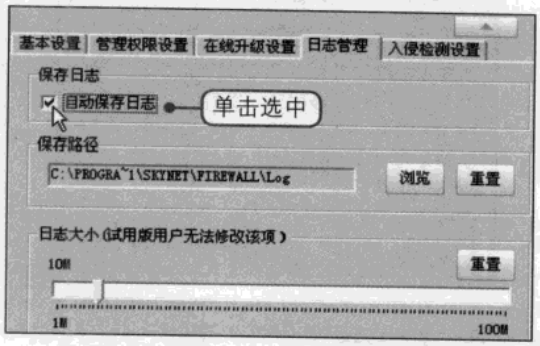
10 在线升级设置

①单击“在线升级设置”标签切换至该选项卡。②单击选中“在设定的时间段内不提示” 单选按钮。③设置时间段，例如单击选中“半个月”单选按钮。



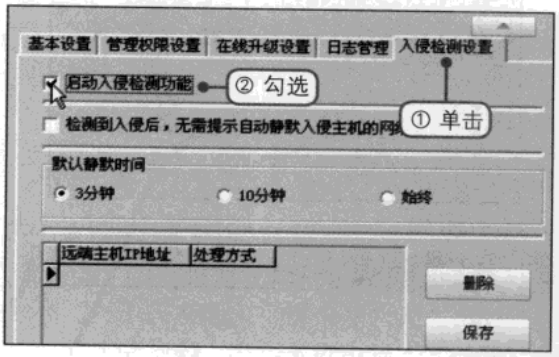
11 日志管理

单击“日志管理”标签切换至该选项卡，在“保存日志”选项组中勾选“自动保存日志”复选框。用户可在“保存路径”选项组中设置保存路径。



12 入侵检测设置

①单击“入侵检测设置”标签切换至该选项卡下。②勾选“启动入侵检查功能”复选框。最后单击“确定”按钮应用设置。



13 设置安全级别

返回天网防火墙主界面，用户可在主界面下设置安全级别，例如单击“中”选项。

14 查看设置后的防火墙

滑块自动滑到“中”选项处，此时可在主界面窗口中看见设置后的天网防火墙。

3.5 禁止可移动硬盘自动运行

当用户将可移动硬盘与电脑连接后，有时可移动硬盘会自动运行，这样一来，若该移动硬盘中含有病毒或者木马则会直接进入电脑，对电脑造成破坏，因此用户应当禁止可移动硬盘自动运行。

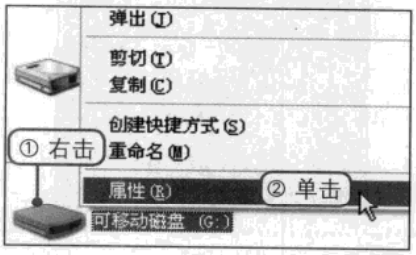
禁止可移动硬盘自动运行的具体操作步骤如下。

① 打开“我的电脑”窗口

双击桌面上“我的电脑”快捷图标，打开“我的电脑”窗口。

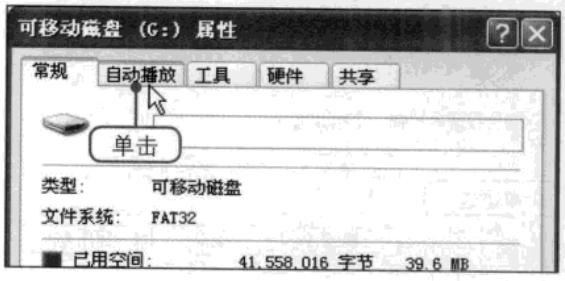
② 单击“属性”命令

①右击“可移动磁盘”图标。②在弹出的快捷菜单中单击“属性”命令。



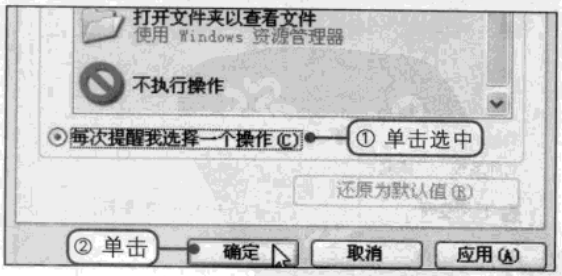
③ 切换至“自动播放”选项卡

打开“可移动磁盘（G：）属性”对话框，单击“自动播放”标签切换至“自动播放”选项卡。



④ 禁止自动运行

①在“自动播放”选项卡单击选中“每次提醒我选择一个操作”单选按钮。②选中后单击“确定”按钮保存退出即可。



3.6 禁止光盘自动运行

用户除了将有关的数据存储在可移动硬盘中外，还常常会存储在光盘中，但在使用光盘的时候也难免遭到病毒和木马的攻击，因此同样需要设置禁止光盘的自动运行。

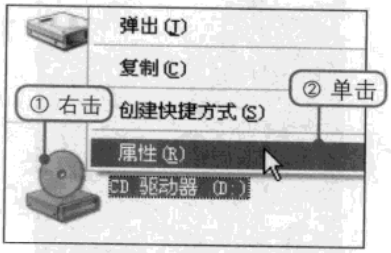
禁止光盘自动运行的具体操作步骤如下。

① 打开“我的电脑”窗口

双击桌面上“我的电脑”快捷图标，打开“我的电脑”窗口。

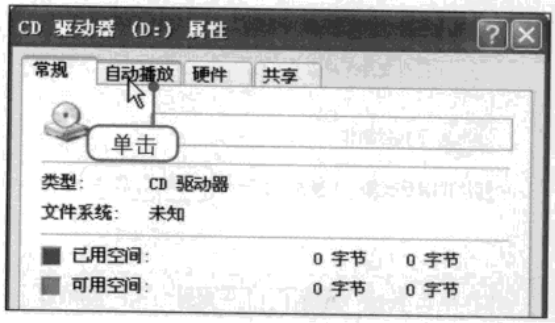
② 单击“属性”命令

①右击“CD驱动器”图标。②在弹出的快捷菜单中单击“属性”命令。



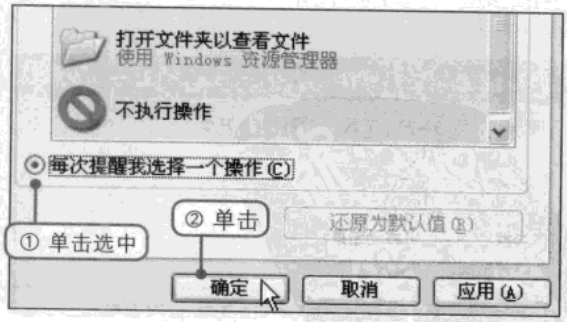
③ 切换至“自动播放”选项卡

打开“CD驱动器（D：）属性”对话框，单击“自动播放”标签切换至“自动播放”选项卡。



④ 禁止自动运行

①在“自动播放”选项卡下单击选中“每次提醒我选择一个操作”单选按钮。②选中后单击“确定”按钮保存退出即可。



Chapter 04

修复系统漏洞

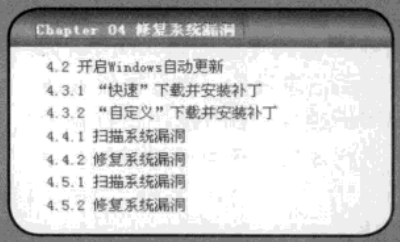
重点知识

1. 认识系统漏洞
2. 开启Windows自动更新
3. 通过微软官方网站下载补丁
4. 使用360安全卫士修复系统漏洞
5. 使用超级兔子修复系统漏洞

系统漏洞往往被网络上的不法分子或者电脑黑客所利用，通过植入病毒、木马等方式来攻击或控制整个电脑，从而窃取用户电脑中的重要资料和信息，甚至破坏用户的系统，导致重要数据丢失、系统瘫痪。用户可通过开启Windows自动更新和登录微软官网下载并安装升级补丁来修复系统漏洞；另外，用户也可以使用360安全卫士或者超级兔子等第三方软件来自动修复系统漏洞。

视频文件

参见随书光盘：视频教程\Chapter 04



4.1 认识系统漏洞

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，这个缺陷或错误很有可能被不法者或者黑客利用，通过植入病毒等方式来攻击整个电脑，从而窃取电脑中的重要资料或信息，甚至使操作系统瘫痪。黑客们经常就是利用操作系统中的漏洞来攻击和入侵用户电脑的。

4.1.1 什么是系统漏洞

系统漏洞也可以是某个程序（包括操作系统）在设计时未考虑周全，当程序遇到一个表面上看似合理，但是实际无法处理的问题时引发的不可预见的错误。它对用户造成的不良后果如下所述。

- 对用户操作造成不便，如不明原因的死机和丢失文件等。
- 系统漏洞被恶意用户利用，造成信息泄漏，如黑客攻击网站就是利用了网络服务器操作系统的漏洞。

系统漏洞产生的原因大致有以下3个原因。

- 编程人员的人为因素，在程序编写过程，为实现不可告人的目的，在程序代码的隐蔽处保留后门。
- 由于编程人员的能力、经验和当时的安全技术所限制，在程序中难免会有不足之处，轻则影响程序的运行效率，重则导致其他用户利用此漏洞大作文章。
- 由于硬件原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现出来。

4.1.2 Windows系统中常见的系统漏洞

Windows系统漏洞层出不穷也有其客观原因，作为应用于桌面的操作系统——Windows也是如此，且由于其在桌面操作系统的垄断地位，使其存在的问题会很快暴露。此外，与Linux等开放源码的操作系统相比，Windows属于暗箱操作，普通用户无法获取源代码，因此安全问题均由微软自身解决。

在Windows XP中常见的系统漏洞如下。

1 UPNP缓冲溢出漏洞

Windows XP默认启动的UPNP(Universal Plug and Play)服务存在严重的安全问题，UPNP体系面向无线设备、PC机和智能应用，提供普遍的对等网络连接，在家用信息设备、办公网络设备间提供了TCP/IP连接和Web访问功能，该服务可用于检测和集成UPNP硬件。UPNP协议存在的安全漏洞，可使攻击者能非法获取任何Windows XP的系统级访问、进行攻击、还可通过控制多台Windows XP操作系统电脑发起分布式的攻击。

建议用户禁用UPNP服务或者通过登录微软官方网站下载补丁程序。

2 升级漏洞程序

例如将Windows XP升级到Windows XP Pro，IE 6.0会重新安装，以前的补丁程序将会被全部清除。

Windows XP操作系统的升级程序不仅会删除IE的补丁文件，还会导致微软的升级服务器无法正确识别IE是否存在缺陷，即Windows XP Pro系统存在某些网页或者HTML邮件的脚本可自动调用Windows的程序以及可通过IE漏洞窥视用户电脑中的文件这两个潜在威胁。

建议用户登录微软官方网站下载最新的IE浏览器升级补丁。

3 帮助和支持中心漏洞

用户可通过帮助和支持中心提供的集成工具获取针对各种主题的帮助和支持，在目前版本的Windows XP帮助和支持中心存在漏洞，该漏洞使攻击者可跳过特殊的网页（在打开该网页时，调用错误的函数，并将存在的文件或文件夹的名字作为参数传送）来使上传文件或文件夹的操作失败，随后该网页可在网站上公布，用来攻击访问该网站的用户或者被作为邮件传播来攻击。该漏洞除使攻击者可删除文件外，不会赋予其他权利，攻击者既无法获取系统管理员的权限，也无法读取或修改文件。

建议用户安装Windows XP的Service Pack 1。

4 压缩文件漏洞

攻击者可通过该漏洞的Windows XP压缩文件夹按攻击者的选择运行代码。

在安装“Plus!”包的Windows XP系统中，“压缩文件夹”功能允许将后缀名为Zip文件作为普通文件夹处理。“压缩文件夹”功能存在两个漏洞，即在解压缩Zip文件时存在于被解压文件中未经检查的缓冲很可能导致浏览器崩溃或者攻击者的代码被运行以及解压缩功能在非用户指定目录中放置文件导致攻击者在用户系统的已知位置中放置文件。

建议用户不接受不信任的邮件附件，也不下载不信任的文件。

5 服务拒绝漏洞

Windows XP支持点对点的协议（PPTP），是作为远程访问服务实现的虚拟专用网技术，由于在控制用于建立、维护和拆开PPTP连接的代码段中存在未经检查的缓存，因此导致Windows XP的实现中存在漏洞。通过向一台存在该漏洞的服务器发送不正确的PPTP控制数据，攻击者可损坏核心内存并导致系统失效，中断所有系统中正在运行的进程。该漏洞可攻击任何一台提供PPTP服务的服务器，对于PPTP客户端的工作站，攻击者只需激活PPTP会话即可进行攻击。对任何遭到攻击的系统，可通过重启来恢复正常操作。

建议用户不默认启动PPTP。

6 Windows Media Player漏洞

该漏洞可能导致用户信息的泄漏，脚本调用，缓存路径泄漏。

Windows Media Player漏洞主要产生两个问题：一是信息泄漏漏洞，它给攻击者提供了一种可在用户系统上运行代码的方法；二是脚本执行漏洞，当用户选择播放一个特殊的媒体文件，接着又浏览一个特殊建造的网页后，攻击者就可利用该漏洞运行脚本，由于该漏洞有特别的时序要求，因此利用该漏洞进行攻击相对就比较困难。

Windows Media Player的信息泄漏漏洞不会影响在本地机器上打开的媒体文件。因此建议用

户将要播放的文件先下载到本地电脑上再播放，这样就可以不受到利用此漏洞进行的攻击。对于脚本执行漏洞，只有完全按下面的顺序进行一系列操作，攻击者才有可能利用该漏洞进行一次成功攻击。具体的操作如下：用户必须播放位于攻击者那边的一个特殊媒体文件，播放该特殊文件后，该用户必须关闭Windows Media Player而不再播放其他文件，接着用户必须浏览一个由攻击者构建的网页。因此用户只要不按照前面介绍的顺序进行操作即可不受到攻击。

7 RDP漏洞

Windows操作系统通过RDP（Remote Desktop Protocol，远程桌面协议）为客户端提供远程终端会话。RDP 协议将终端会话的相关硬件信息传送至远程客户端，其漏洞包括与某些RDP版本的会话加密实现有关的漏洞以及与Windwos XP中的RDP实现对某些不正确的数据包处理方法有关的漏洞。

Windows XP 默认并未启动它的远程桌面服务。即使远程桌面服务启动，只需在防火墙中屏蔽3389端口，即可避免该攻击。

8 VM漏洞

VM（Microsoft Java Virtual Machine，微软Java虚拟机）漏洞可能造成信息泄漏，并执行攻击者的代码。攻击者可通过向JDBC（Java Data Base Connectivity，Java数据库连接）类传送无效的参数使宿主应用程序崩溃，攻击者需在网站上拥有恶意的Java applet 并引诱用户访问该站点。 恶意用户可在用户机器上安装任意DLL，并执行任意的本机代码，潜在地破坏或读取内存数据。

建议用户经常进行相关软件的安全更新。

9 热键漏洞

热键功能是系统提供的服务，当用户离开计算机后，该计算机即处于未保护状况下，此时Windows XP会自动实施“自注销”，虽然无法进入桌面，但由于热键服务还未停止，仍可使用热键启动应用程序。设置热键后，由于Windows XP的自注销功能，可使系统“假注销”，其他用户即可通过热键调用程序。

建议用户启用屏幕保护程序并设置密码，离开电脑时锁定电脑。

10 账号快速切换漏洞

Windows XP设计了账号快速切换功能，使用户可快速地在不同的账号间切换，但其设计存在问题，可被用于造成账号锁定，使所有非管理员账号均无法登录。

配合账号锁定功能，用户可利用账号快速切换功能，快速重试登录另一个用户名，系统则会判别为暴力破解，从而导致非管理员账号锁定。

建议用户暂时禁止账号快速切换功能。

什么是漏洞

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。漏洞表现在软件编写存在BUG、系统配置不当、口令失窃、嗅探未加密通讯技术及设计存在缺陷等方面。

4.2 开启Windows自动更新

Windows XP操作系统自带了“自动更新”工具，该工具为系统定期检查重要更新，并及时为用户安装更新文件，但前提是要开启自动更新功能。自动更新工具为用户提供了自动更新、自定义安装、通知用户下载和关闭自动更新四种选择，用户可根据自身的实际情况进行选择。

① 打开“控制面板”窗口

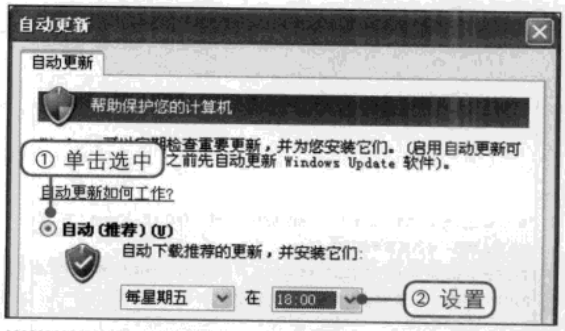
①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“控制面板”命令，打开“控制面板”窗口。

② 打开“自动更新”对话框

在“控制面板”窗口中双击“自动更新”图标，打开“自动更新”对话框。

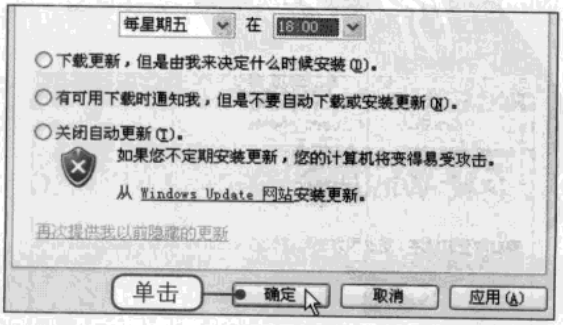
③ 设置自动更新选项

①在“自动更新”对话框中选择自动更新的方式，例如单击选中“自动”单选按钮即可自动下载推荐的更新，并进行安装。②在下方设置具体的自动更新时间。



④ 单击“确定”按钮

设置完毕后单击“确定”按钮关闭对话框即可，系统会按照用户设置的时间进行及时的自动更新。



4.3 通过官方网站下载并安装补丁

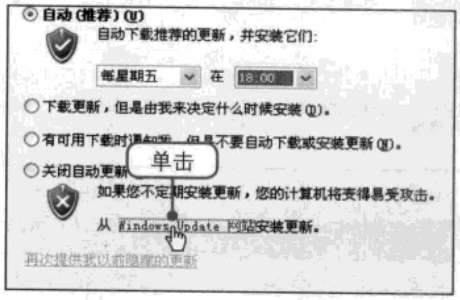
用户如果觉得Windows自动更新修复系统漏洞较慢，可选择通过微软官方网站下载升级补丁。可以直接登录微软官方网站下载升级补丁，也可以在“自动更新”对话框中打开对应的网站下载升级补丁。

4.3.1 “快速”下载并安装补丁

在“自动更新”对话框的底部单击“Windows Update网站”文字链接打开对应的网站，打开网站后需要安装控件方可继续操作。接着就可下载并安装补丁，可选择“快速”方式下载并安装补丁，该方式只查找和安装适合用户电脑的最重要的更新程序。

① 打开Windows Update网站

按照上一节介绍的方法打开“自动更新”对话框，在该对话框中单击“Windows Update网站”文字链接，打开Windows Update网站。



② 选择“快速”方式查找更新程序

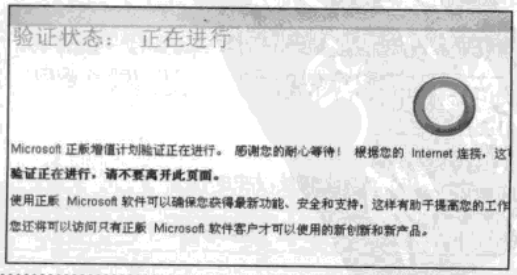
在弹出的浏览器窗口中可选择查看电脑更新程序的方式。例如单击“快速”按钮选择“快速”方式查找更新程序。

③ 正版Windows验证

用户在获取更新程序之前需要进行正版Windows验证，在打开的网页中直接单击“继续”按钮开始验证。

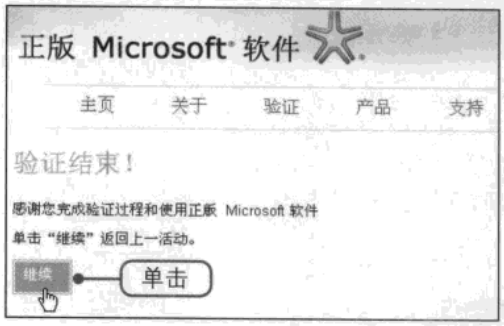
④ 查看验证状态

页面转换至验证状态，此时正在进行验证操作，请耐心等待。



⑤ 验证成功

验证结束后转换至“验证结束”界面，验证成功，单击“继续”按钮。



⑥ 再次单击“快速”按钮

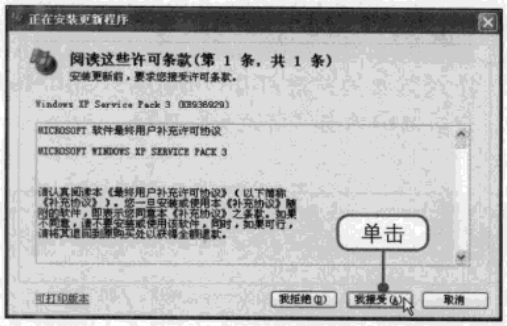
页面返回至初始界面，再次单击“快速”按钮开始查找适合电脑最重要的更新程序。

⑦ 单击“安装更新程序”按钮

查看一段时间后打开“快速结果”界面，此时可在页面中看见查找的结果，单击“安装更新程序”按钮开始安装。

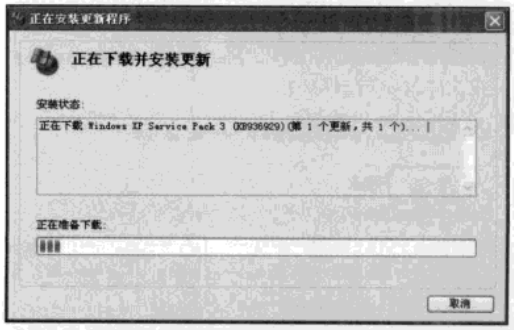
⑧ 接受许可协议

弹出“正在安装更新程序”对话框，阅读对话框中的许可条款后单击“我接受”按钮。



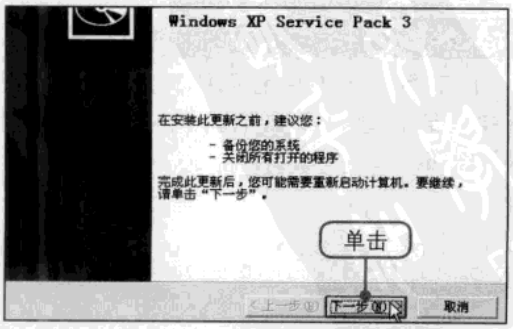
⑨ 下载并安装更新程序

打开“正在下载并安装更新”界面，此时可以看见下载更新程序的进度，请耐心等待。



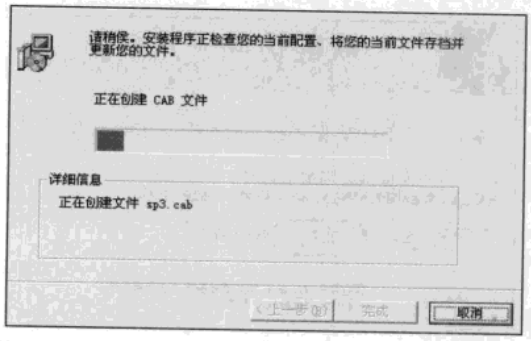
⑩ 开始安装

安装到一半左右的时候弹出“软件安装向导”对话框，直接单击“下一步”按钮。



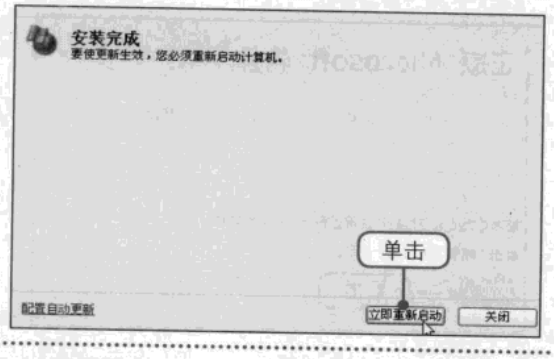
⑪ 查看安装进度

打开“正在更新您的系统”界面，此时可以看见安装更新程序的进度，请耐心等待。



⑫ 安装完成

打开“安装完成”界面，提示用户必须重启计算机，单击“立即重新启动”按钮即可。



4.3.2 “自定义”下载并安装补丁

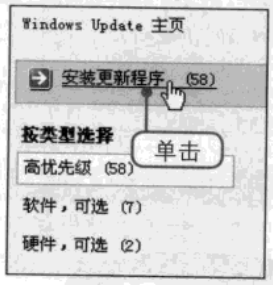
由于“快速”方式只查找和安装适合用户电脑的最重要的更新程序，因此用户可在使用了“快速”方式之后再次使用“自定义”方式查找并安装适合用户电脑的所有更新程序。

① 单击“自定义”按钮

按照前面的方法打开Windows Update网站，在页面中单击“自定义”按钮。

② 选择需要安装更新的程序

在打开的页面中用户可手动选择需要安装的更新程序，建议全部安装。单击页面左侧的“安装更新程序”文字链接。

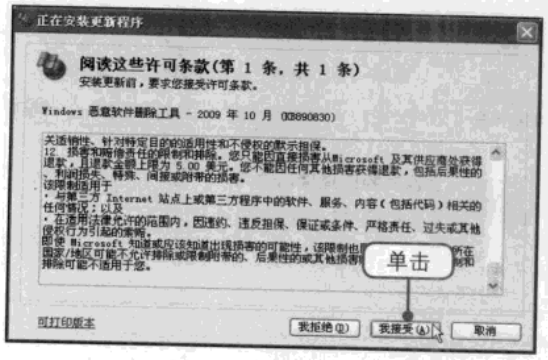


③ 单击“安装更新程序”按钮

此时可在页面中看见所有的更新程序已经被勾选，直接单击上方的“安装更新程序”按钮。

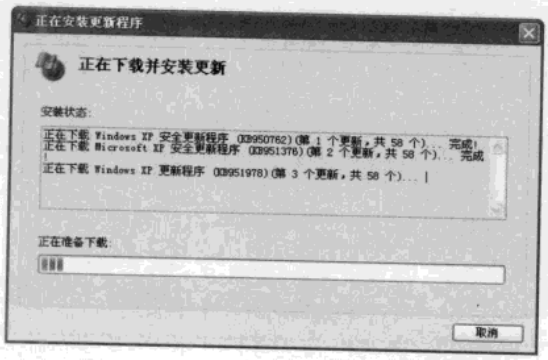
④ 阅读许可条款

弹出“正在安装更新程序”对话框，阅读许可条款后单击“我接受”按钮。



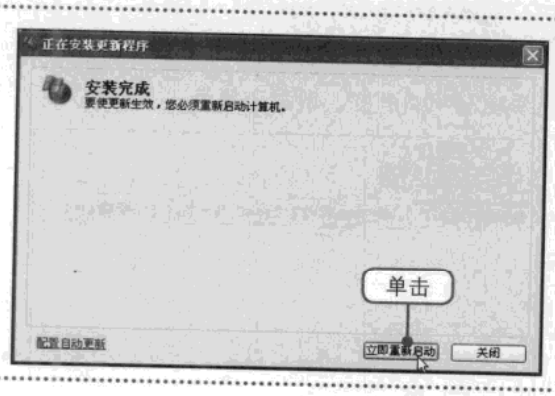
⑤ 开始安装

打开“正在下载并安装更新”界面，此时可以看见下载更新程序的进度，只需耐心等待即可。



⑥ 安装完成

安装完成后跳转至“安装完成”界面，单击“立即重新启动”按钮重启电脑即可。



4.4 使用360安全卫士修复系统漏洞

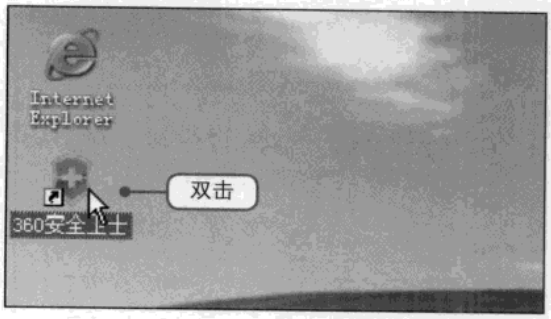
可以使用第三方软件来修复系统漏洞，360安全卫士是一款由奇虎公司推出的完全免费（奇虎官方声明：“我们永久免费”）的安全类上网辅助软件，它不仅拥有修复系统漏洞的功能，而且还具有恶意软件清理、木马查杀、电脑全面体检、垃圾和痕迹清理以及系统优化等功能。本节以360安全卫士V6.0.2版本为例进行介绍。

4.4.1 扫描系统漏洞

可以使用360安全卫士扫描电脑系统中的所有漏洞，其中包括Windows、IE、DirectX、Jscript 以及office办公软件等补丁。

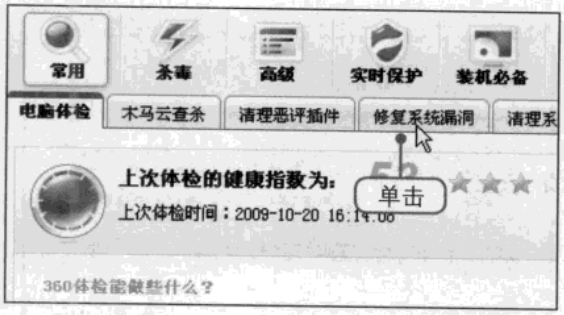
① 启动360安全卫士

下载并安装好360安全卫士之后，在桌面上双击“360安全卫士”快捷图标。



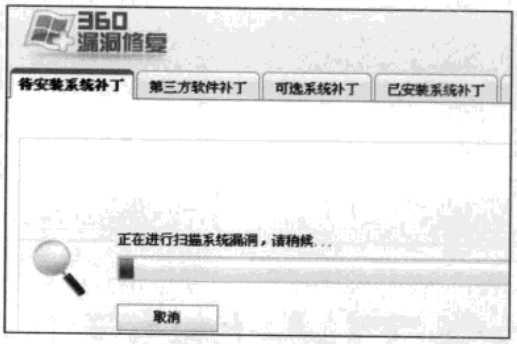
② 切换至“修复系统漏洞”选项卡

打开“360安全卫士”主界面窗口，单击“修复系统漏洞”标签切换至该选项卡。



③ 扫描系统漏洞

打开360漏洞修复窗口，此时可以看见扫描系统漏洞的进度，请耐心等待。



④ 查看扫描的结果

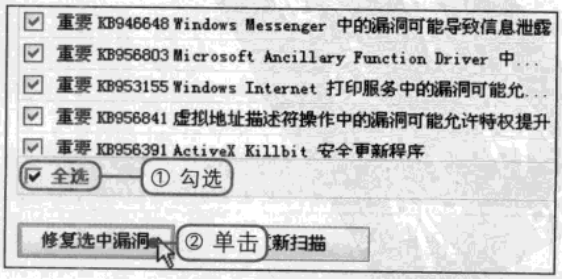
扫描完毕后切换至新的界面，用户可在界面中查看系统存在的漏洞。

4.4.2 修复系统漏洞

360安全卫士扫描出系统中存在的漏洞之后，用户就可以直接使用该软件下载并安装对应的补丁。

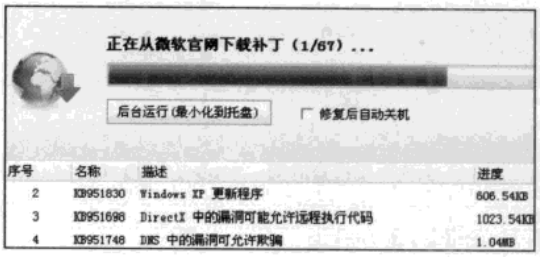
① 选中全部漏洞

①在上一小节扫描完毕后打开的界面中勾选“全选”复选框。②单击“修复选中漏洞”按钮。



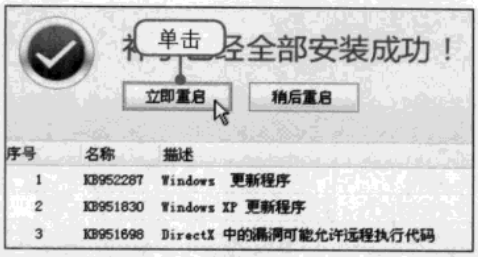
② 开始修复漏洞

在打开的界面中可以看见360软件正在从微软官方网站下载补丁。



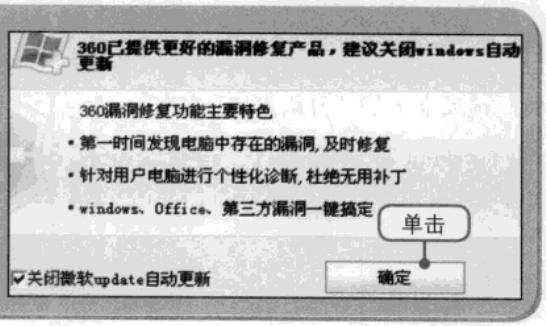
③ 修复完毕

耐心等待一段时间之后，补丁会全部安装成功，单击“立即重启”按钮重新启动电脑即可。



使用360安全卫士修复漏洞时需要关闭系统自动更新

当用户开启自动更新并初次使用360安全卫士修复系统漏洞时，会弹出提示用户关闭自动更新的提示框。



4.5 使用超级兔子修复系统漏洞

超级兔子可以说是一款完整的系统维护工具，它不但可以清理电脑中大多数的垃圾文件、注册表中的垃圾，而且还可以优化、设置系统中大多数的选项，打造一个属于自己的Windows系统。使用超级兔子还可以扫描并修复系统中存在的漏洞。

4.5.1 扫描系统漏洞

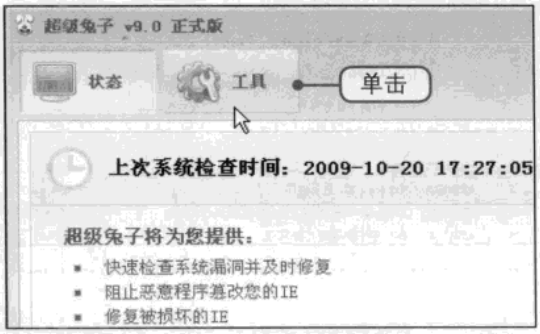
用户使用超级兔子扫描系统漏洞时需要启动升级天使，然后可使用该软件扫描系统中存在的所有漏洞。

① 启动超级兔子

下载并安装好超级兔子之后，便可双击桌面上的“超级兔子”快捷图标。

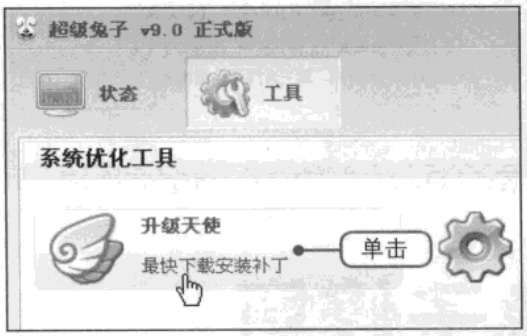
② 单击“工具”按钮

打开“超级兔子V9.0正式版”窗口，单击“工具”按钮。



③ 启动升级天使

在超级兔子工具窗口中单击“系统优化工具”选项卡下的“升级天使”按钮。

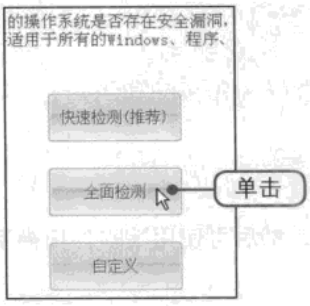


④ 单击“Windows升级补丁”按钮

打开“升级天使”界面，单击左侧的“Windows升级补丁”按钮。

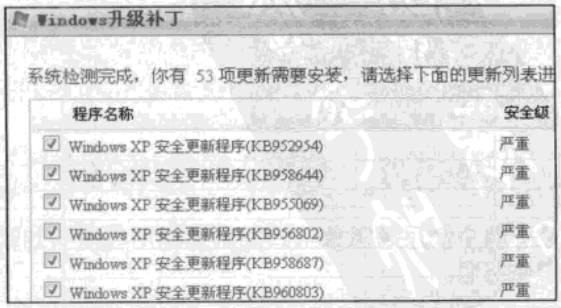
⑤ 单击“全面检测”按钮

在窗口中部选择检测系统漏洞的方式，例如单击“全面检测”按钮。



⑥ 查看检测的结果

耐心等待一段时间之后，用户可在打开的窗口中看见检测的结果。

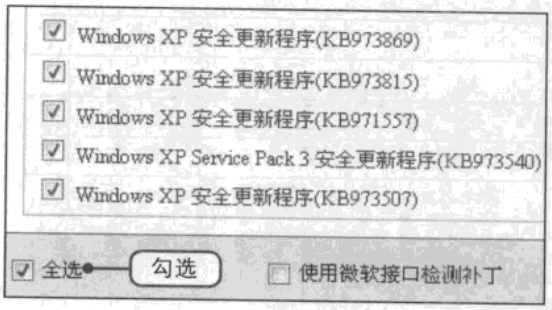


4.5.2 修复系统漏洞

使用超级兔子检测出系统的漏洞之后就可以在升级天使窗口中勾选扫描出的全部漏洞并开始下载安装对应的补丁。

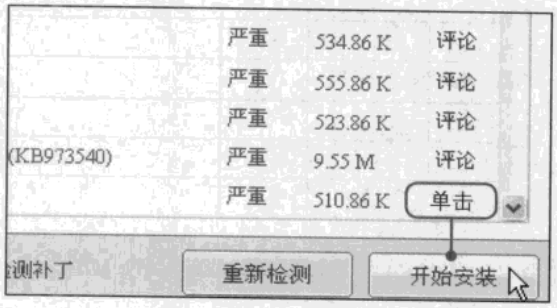
① 全部选中

在检测出系统漏洞的窗口底部勾选“全选”复选框，即可全部选中检测的漏洞。



② 单击“开始安装”按钮

单击右侧的“开始安装”按钮开始修复系统漏洞。

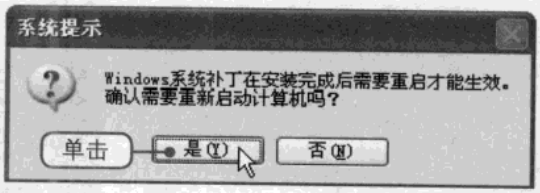


③ 查看修复的进度

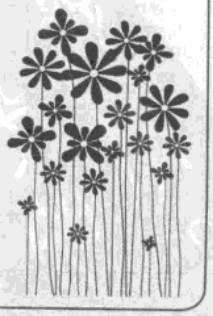
此时可在“下载状态”选项卡下查看系统漏洞修复的进度，请耐心等待。

④ 重启计算机

修复完毕后弹出“系统提示”对话框，提示用户需要重启后方可生效，单击“是”按钮。



读书笔记



Chapter 05

安全使用文件与应用软件

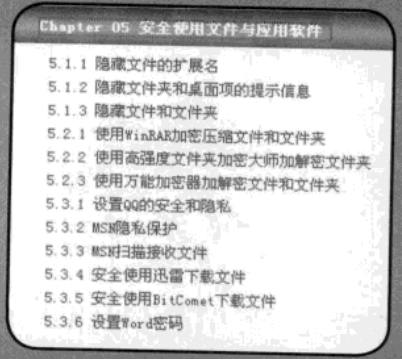
重点知识

1. 隐藏文件或文件夹
2. 加密文件和文件夹
3. 应用软件安全设置

使用电脑时要安全地使用文件与应用软件，对于电脑中的重要文件或者文件夹，可以通过一些设置将它们隐藏，还可以使用不同的方法将它们加密以保障其安全性，如使用WinRAR解压缩软件、高强度文件夹加密大师和万能加密器等软件。对于常用的应用软件同样也需要进行安全设置，如对Word、Excel办公软件进行加密，对QQ、MSN和下载软件进行安全设置等。

视频文件

参见随书光盘：视频教程\Chapter 05



5.1 隐藏文件或文件夹

可以通过不同层次的隐藏方式将保存在电脑中的重要文件和文件夹隐藏，如隐藏扩展名、提示信息、整个文件和文件夹。用户可根据文件的重要性选择其隐藏方式。

5.1.1 隐藏文件的扩展名

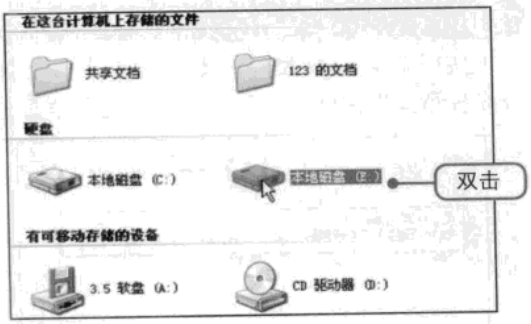
对某一文件或者文件夹进行重命名操作时，往往会不小心把该文件或文件夹的扩展名删除掉，重新命名之后发现该文件无法打开。可以通过设置将文件和文件夹的扩展名隐藏来避免这种情况的发生。

① 打开“我的电脑”窗口

在桌面上双击“我的电脑”图标，打开“我的电脑”窗口。

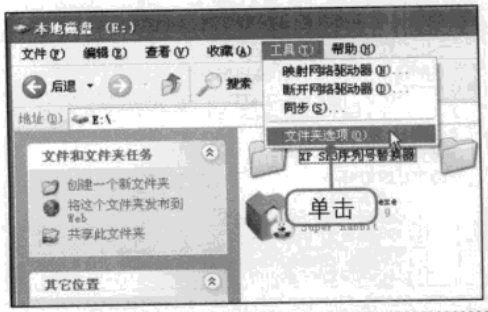
② 查看显示扩展名的文件或文件夹

在“我的电脑”窗口中打开任意一个磁盘查看显示扩展名的文件或者文件夹，例如双击“本地磁盘（E:）”图标。



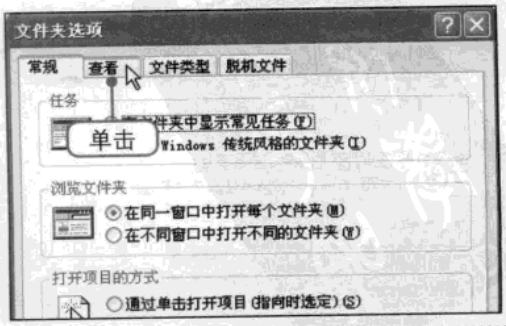
③ 单击“文件夹选项”命令

在E盘窗口中可以看见显示扩展名的文件，单击窗口菜单栏中的“工具>文件夹选项”命令。



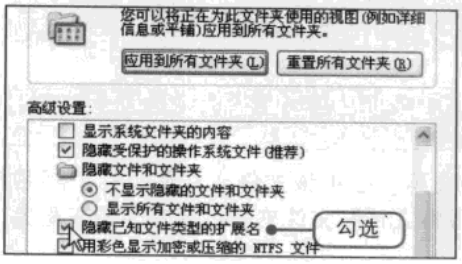
④ 切换至“查看”选项卡

打开“文件夹选项”对话框，单击“查看”标签切换至该选项卡。



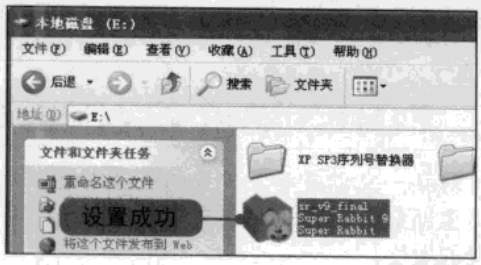
⑤ 隐藏已知文件类型的文件名

在“高级设置”列表框中勾选“隐藏已知文件类型的扩展名”复选框，然后单击下方的“确定”按钮。



⑥ 隐藏成功

返回“本地磁盘（E:）”窗口，此时可以看见文件的扩展名已经被隐藏。

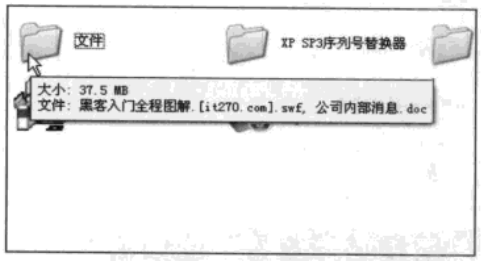


5.1.2 隐藏文件夹和桌面项的提示信息

当将鼠标靠近某一个文件或者文件夹时，在鼠标下方会显示其相关信息，不用打开文件夹就可知道里面的内容，这种情况下用户可通过设置将其提示信息进行隐藏。

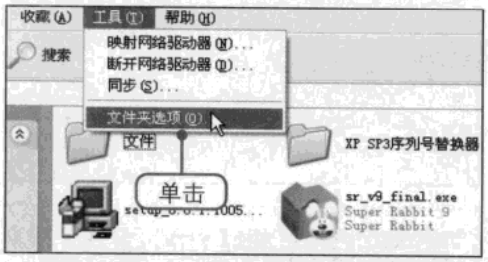
① 查看显示提示信息的文件夹

按照前面的步骤打开本地磁盘E，将鼠标放在任意文件夹图标上可以看见其提示信息。



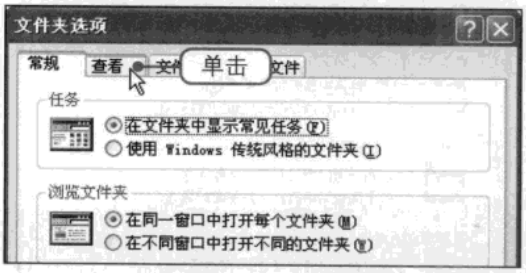
② 单击“文件夹选项”命令

单击窗口菜单栏中的“工具>文件夹选项”命令。



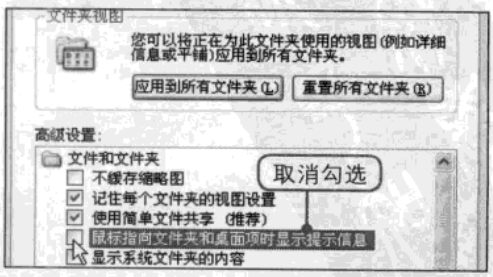
③ 切换至“查看”选项卡

打开“文件夹选项”对话框，单击“查看”标签切换至该选项卡。



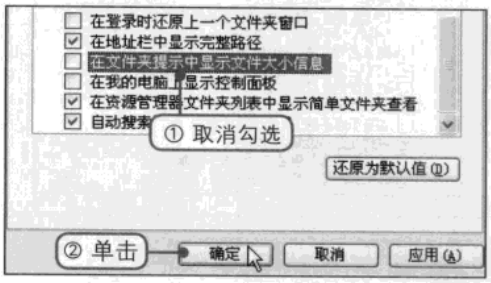
④ 隐藏文件夹提示信息

取消勾选“高级设置”列表框中的“鼠标指向文件夹和桌面项时显示提示信息”复选框。



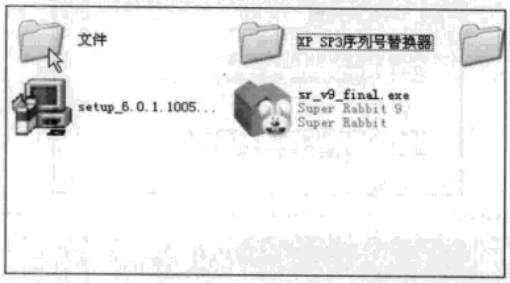
⑤ 隐藏文件大小

向下滑动列表框右侧的滚动条，①取消勾选“在文件夹提示中显示文件大小信息”复选框。②单击“确定”按钮。



⑥ 查看设置后的文件夹

返回“本地磁盘(E:)”窗口，将鼠标移动到步骤1中的文件夹时，此时可以看见并无任何提示信息，即设置成功。

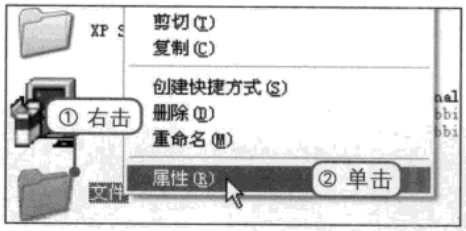


5.1.3 隐藏文件和文件夹

可以直接隐藏该文件或者文件夹，使其不在窗口中显示，从而保证文件的安全性。

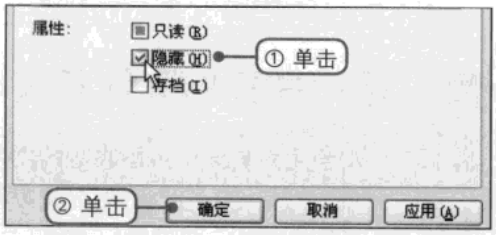
① 单击“属性”命令

①右击需要隐藏的文件夹，②在弹出的快捷菜单中单击“属性”命令。



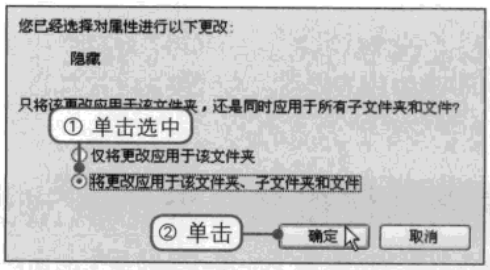
② 设置文件夹属性为隐藏

弹出“文件属性”对话框，①勾选“隐藏”复选框。②单击“确定”按钮。



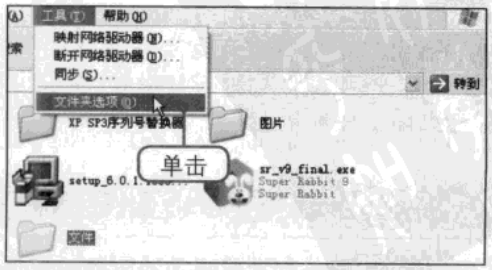
③ 确认更改属性

弹出“确认属性更改”对话框，①单击选中“将更改应用于该文件夹、子文件夹和文件”单选按钮。②单击“确定”按钮。



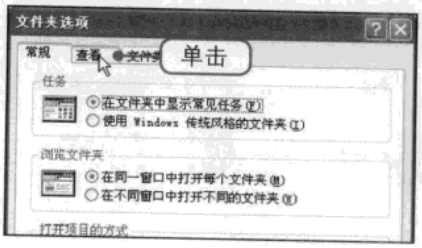
④ 单击“文件夹选项”命令

返回窗口，此时可以看见隐藏的文件夹呈透明状。单击菜单栏中的“工具>文件夹选项”命令。



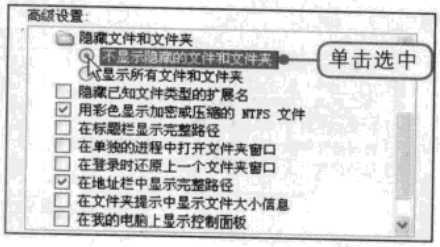
⑤ 切换至“查看”选项卡

打开“文件夹选项”对话框，单击“查看”标签切换至该选项卡。



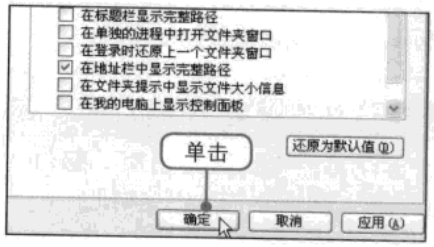
⑥ 不显示隐藏的文件和文件夹

在“高级设置”列表框中单击选中“不显示隐藏的文件和文件夹”单选按钮。



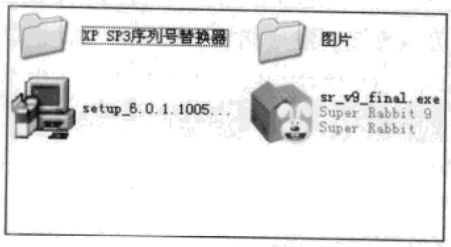
⑦ 单击“确定”按钮

单击“确定”按钮返回隐藏文件所在的窗口。



⑧ 查看设置后的效果

此时可在窗口中看见选中的文件夹“消失”了，即设置成功。



显示所有的文件和文件夹

当用户需要使用被隐藏的文件或者文件夹时，可按照前面的方法打开“文件夹选项”对话框，在“查看”选项卡下的“高级设置”列表框中单击选中“显示所有文件和文件夹”单选按钮即可。

5.2 加密文件和文件夹

当用户在电脑中存储了非常重要的数据时，仅仅隐藏是不够安全的，这就需要使用软件为文件和文件夹进行加密操作，可以使用WinRAR解压缩软件、高强度文件夹加密大师和万能加密器等常用的加密软件。

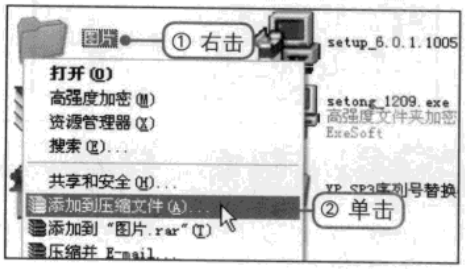
5.2.1 使用WinRAR加密压缩文件和文件夹

WinRAR 是一款功能强大的压缩包管理器，是档案工具 RAR 在 Windows 环境下的图形界

面。用户不仅可以使用它来解压缩从 Internet 上下载的 RAR、ZIP及其他文件，还可以将电脑中文件加密压缩成RAR或ZIP格式的压缩文件。

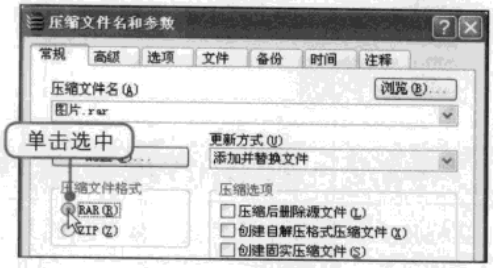
1 单击“添加到压缩文件”命令

打开需要压缩的文件夹所在的磁盘窗口，①右击该文件夹。②在弹出的快捷菜单中单击“添加到压缩文件”命令。



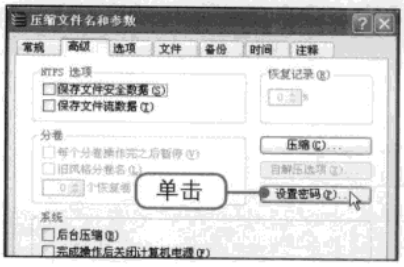
2 设置压缩文件格式

打开“压缩文件名和参数”对话框，在“压缩文件格式”选项组中单击选中RAR单选按钮。



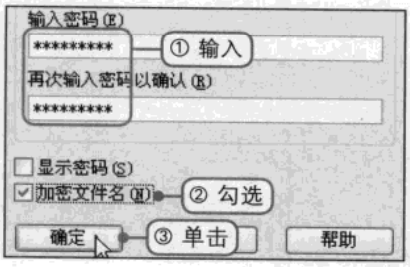
3 单击“设置密码”按钮

单击“高级”标签切换至该选项卡，直接单击“设置密码”按钮。



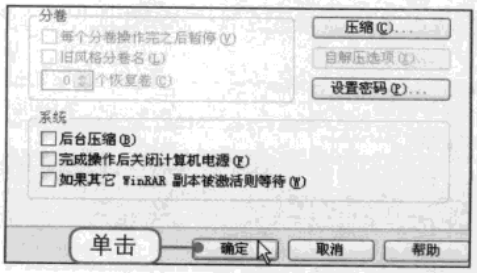
4 设置密码

打开“带密码压缩”对话框，①在文本框中输入设置的密码。②勾选“加密文件名”复选框。③单击“确定”按钮。



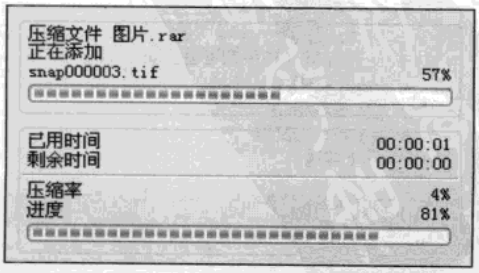
5 开始压缩

返回“压缩文件名和参数”对话框，直接单击“确定”按钮。



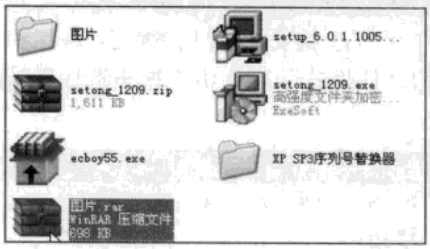
6 查看压缩的进度

弹出“正在创建压缩文件”对话框，此时可以在对话框中看见文件夹压缩的进度，需耐心等待。



⑦ 压缩成功

返回磁盘窗口，用户可以在窗口中看见创建的压缩文件，双击该压缩文件。



⑧ 加密成功

弹出“输入密码”对话框，①在“为加密的文件输入密码”文本框中输入密码。②单击“确定”按钮。

5.2.2 使用高强度文件夹加密大师加解密文件夹

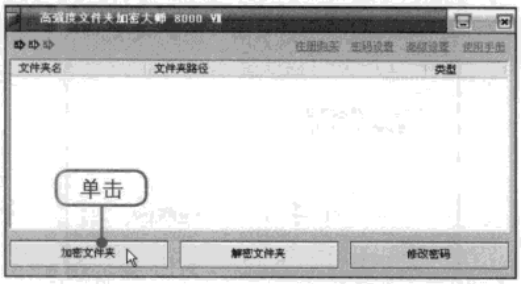
高强度文件夹加密大师是一款专业的文件和文件夹加密器，经过该软件加密的文件夹可以移动至其他电脑上继续使用，即使系统重装和GHOST还原，它依然可以照样使用。

① 启动高强度文件夹加密大师

下载并安装好高强度文件夹加密大师后，双击桌面上对应的快捷图标。

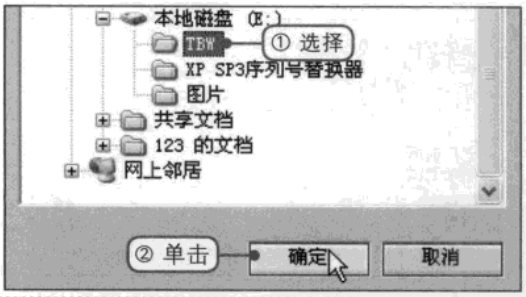
② 单击“加密文件夹”按钮

打开“高强度文件夹大师”主界面窗口，在窗口中单击“加密文件夹”按钮。



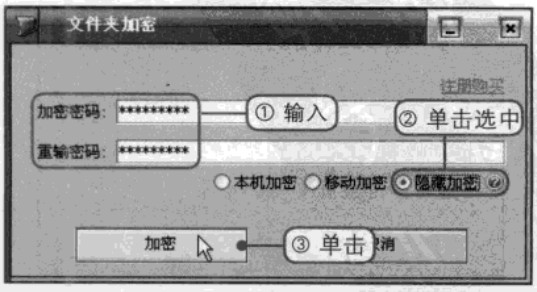
③ 选择需要压缩的文件夹

弹出“浏览文件夹”对话框，①选择需要压缩的文件夹。②单击“确定”按钮。



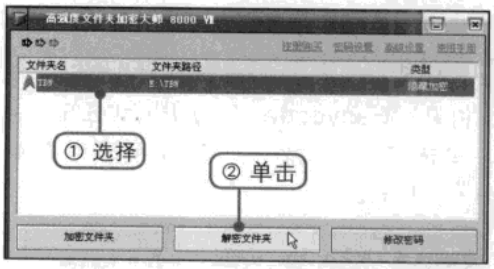
④ 输入设置的密码

①在打开的对话框中输入密码。②单击选中“隐藏加密”单选按钮。③单击“加密”按钮。



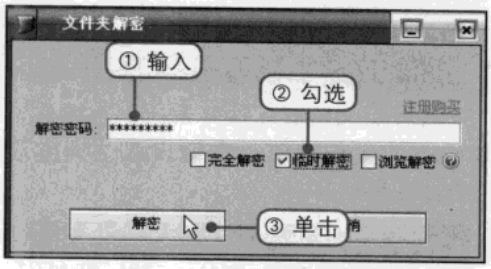
⑤ 查看加密的文件夹

返回“高强度文件夹加密大师”主界面窗口，此时可以看见加密的文件，①选择加密的文件选项。②单击下方的“解密文件夹”按钮。



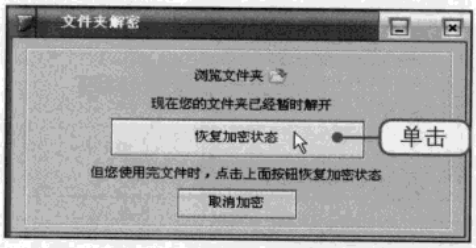
⑥ 输入加密密码

弹出“文件夹解密”对话框，①在“解密密码”文本框中输入步骤4中设置的密码。②勾选“临时解密”复选框。③单击下方的“解密”按钮。



⑦ 恢复加密状态

由于前面选择的是临时解密，当用户关闭加密的文件夹时需要在“文件夹解密”对话框中单击“恢复加密状态”按钮加密刚刚打开的文件夹。



新手学堂 加密的三种方式

高强度文件夹加密大师提供了本机加密、移动加密和隐藏加密三种方式。

- 本机加密的文件安全性极高，该种加密方式可以很好的保护用户电脑的加密数据不被他人使用或者复制到其他电脑中。
- 移动加密的文件既可在本机使用，也可以移动至其他电脑中（包括未安装该软件的电脑）使用，依然保持加密状态。
- 隐藏加密的文件无法在磁盘窗口中显示，用户必须启动该软件后方可在其主界面窗口中进行其他操作。

新手学堂 解密的三种方式

高强度文件夹加密大师同样提供了完全解密、临时解密和浏览解密三种解密方式。

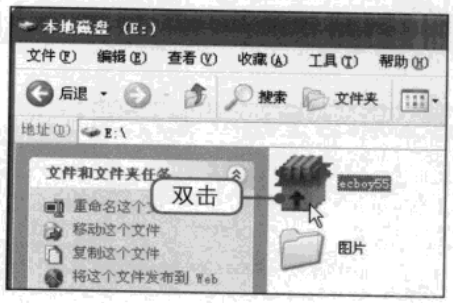
- 完全解密：若用户想彻底地解除密码，可选择此解密方式。
- 临时解密：若用户只是临时地使用加密文件夹中的文件，可选择此种解密方式。
- 浏览解密：使用此种方式解密后自动打开文件夹浏览窗口，待该文件夹窗口关闭后文件自动恢复到加密状态。

5.2.3 使用万能加密器加解密文件和文件夹

万能加密器是一款小巧高速的加密软件，它不限加密文件的大小和类型，加密速度快，安全性能高，不仅拥有加密和解密列表功能，而且还具有独特的密码查询功能。该功能可以使忘记密码的用户重新找到密码。

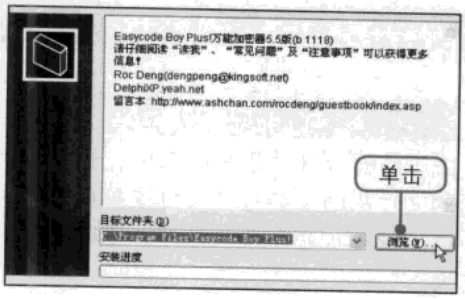
① 启动万能加密器安装程序

下载万能加密器软件并解压到电脑后，打开其所在的磁盘窗口，在窗口双击该安装软件，启动安装程序。



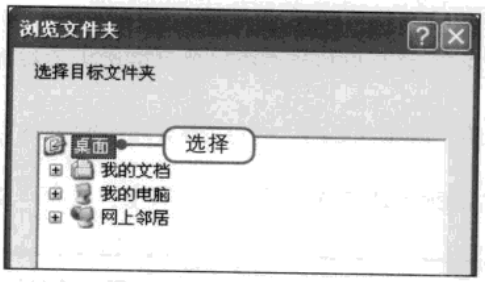
② 单击“浏览”按钮

打开“Easycode Boy Plus! 5.5”对话框，单击“目标文件夹”下拉列表框右侧的“浏览”按钮。



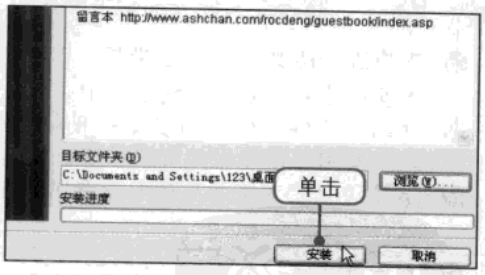
③ 选择安装位置

弹出“浏览文件夹”对话框，由于该软件只有一个EXE文件和记事本，选择“桌面”选项，将其直接安装在桌面上。



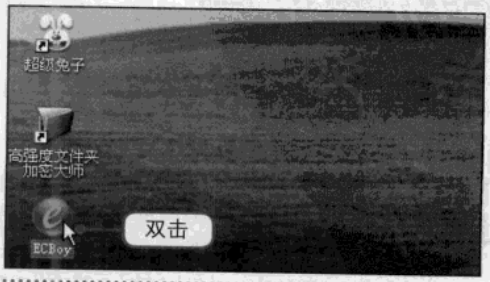
④ 开始安装

单击“确定”按钮返回步骤2中的对话框，直接单击“安装”按钮开始安装。



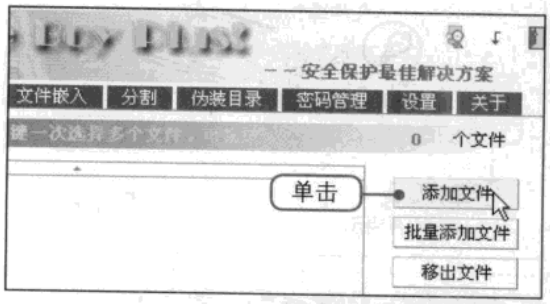
⑤ 启动万能加密器软件

安装完成后可在桌面上看见万能加密器的可执行文件图标和一个名字为“更新”的记事本，双击该快捷图标启动万能加密软件应用程序。



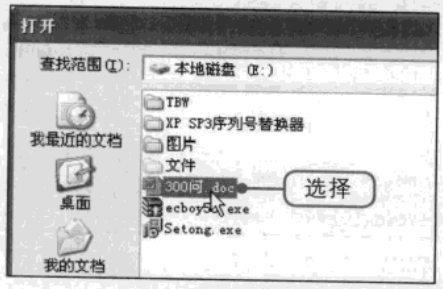
⑥ 单击“添加文件”按钮

打开万能加密器主界面窗口，在“加密”选项卡下单击窗口右侧的“添加文件”按钮。



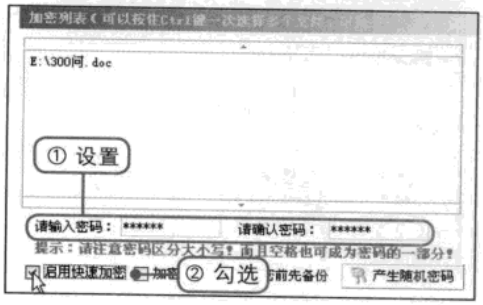
⑦ 添加文件

弹出“打开”对话框，在“查找范围”下拉列表中选择需加密文件所在的磁盘，接着在下方的列表框中选择加密的文件。选中后单击“打开”按钮。



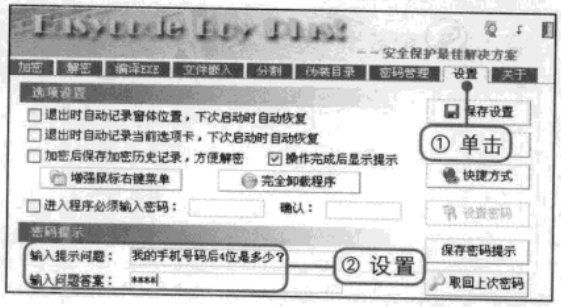
⑧ 输入设置的密码

返回软件主界面窗口，①在“请输入密码”和“请确认密码”文本框中输入设置的密码。②勾选“启动快速加密”复选框。



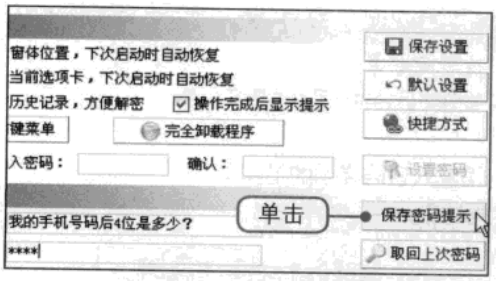
⑨ 设置密码提示

①在窗口中单击“设置”标签切换至该选项卡。②在“密码提示”选项组中输入密码提示问题和问题答案。



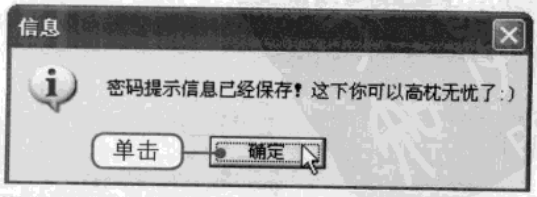
⑩ 保存密码提示

设置完毕后单击右侧的“保存密码提示”按钮保存设置的密码提示。



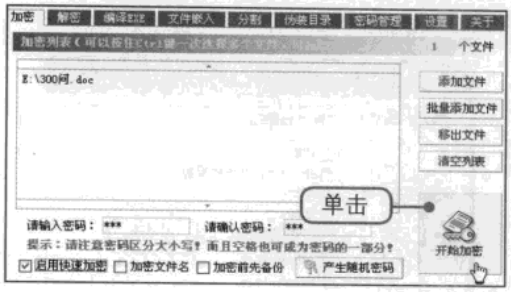
⑪ 保存成功

弹出“信息”提示框，提示用户密码提示信息已经保存。直接单击“确定”按钮。



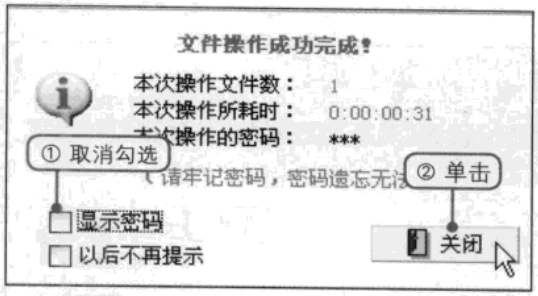
12 开始加密

①单击“加密”标签切换至该选项卡。②在窗口的右下角单击“开始加密”按钮对添加的文件进行加密。



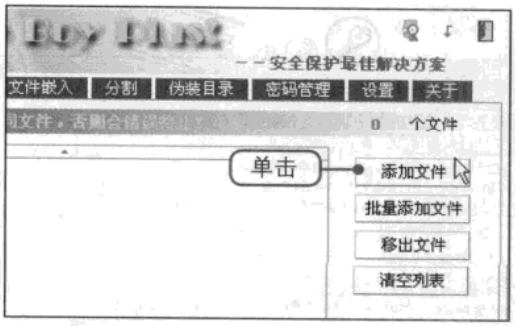
13 加密成功

加密完成后弹出提示框，提示用户文件操作成功完成，①取消勾选“显示密码”复选框。②单击“关闭”按钮。



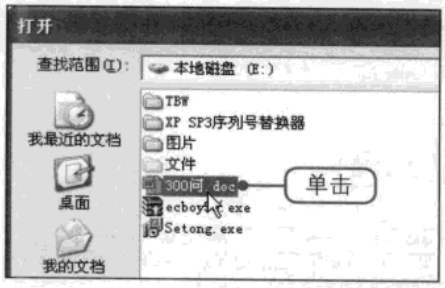
14 单击“添加文件”按钮

用户若需要解密文件时可打开该软件的主界面窗口，在“解密”选项卡中单击窗口右侧的“添加文件”按钮。



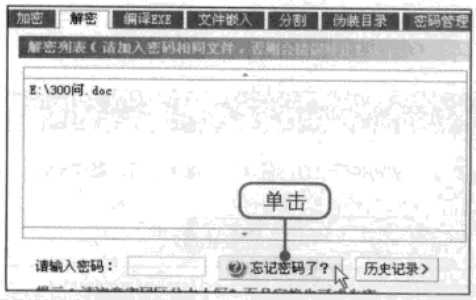
15 添加加密的文件

弹出“打开”对话框，在“查找范围”下拉列表框中选择需加密文件所在的磁盘，接着在下方的列表框中单击加密的文件。



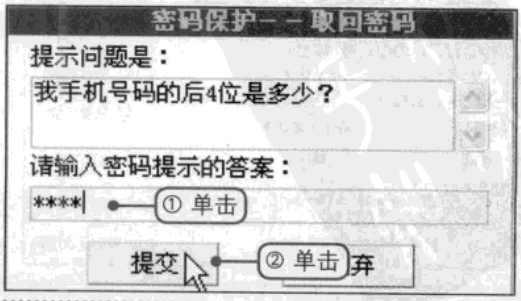
16 单击“忘记密码了？”按钮

单击“打开”按钮返回主界面窗口，可在下方输入密码直接解密，若用户忘记了密码可单击“忘记密码了？”按钮。



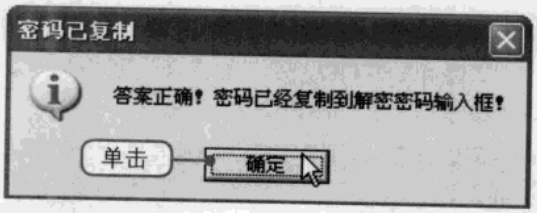
17 输入密码提示问题的答案

弹出“密码保护—取回密码”对话框，①在“请输入密码提示的答案”文本框中输入正确答案。②单击“提交”按钮。



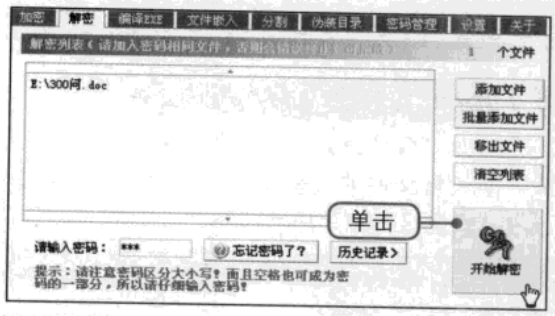
18 获取密码

弹出“密码已复制”提示框，提示用户答案正确，密码已复制到解密密码输入框，直接单击“确定”按钮。



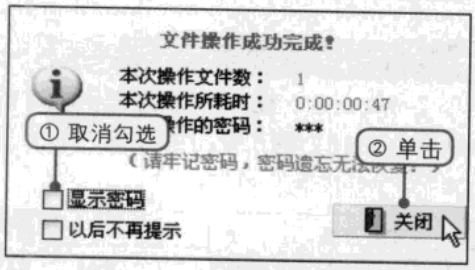
19 开始解密

返回主界面窗口，在“解密”选项卡下单击窗口右下角的“开始解密”按钮。



20 解密成功

解密完成后弹出提示框，提示用户文件操作成功完成，①取消勾选“显示密码”复选框。②单击“关闭”按钮。



5.3 应用软件安全设置

常用的应用软件包括办公软件、下载软件和聊天软件，在使用这些应用软件时，可以对其进行安全设置。例如QQ聊天软件可对其进行安全和隐私的设置；迅雷、Bitcomet等下载软件可直接设置为下载后自动使用杀毒软件扫描；由Word或者Excel所制作的重要文档可通过加密来保障其安全。

5.3.1 设置QQ的安全和隐私

QQ是由腾讯公司开发的一款即时通信软件，用户可以使用该软件和好友进行交流，即时发送和接收信息、自定义图片和照片，在使用QQ之前需要进行安全和隐私的设置，否则聊天记录和相关信息很可能会泄漏。

① 启动腾讯QQ应用软件

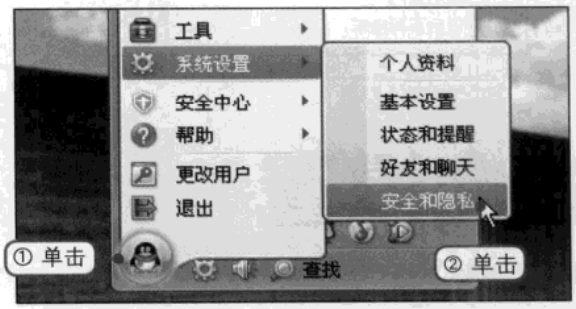
下载并安装QQ之后，在桌面上双击其对应的快捷图标，启动腾讯QQ应用软件。

② 输入账户名和密码

打开QQ用户登录窗口，①输入有效的账户和密码。②输完之后单击右下角的“登录”按钮。

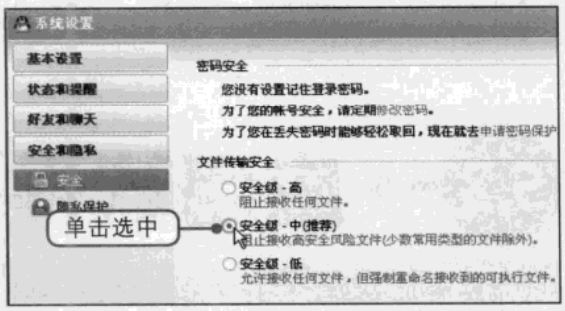
③ 单击“安全和隐私”命令

登录成功之后，①单击QQ主界面左下角的“主菜单”按钮。②在弹出的菜单中单击“系统设置>安全和隐私”命令。



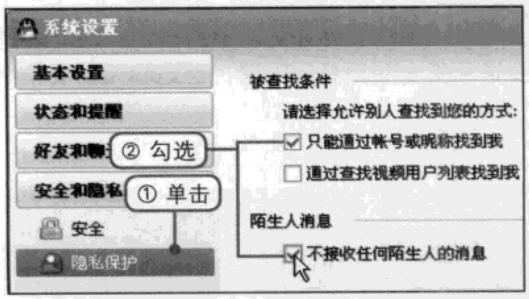
④ 设置文件传输安全

弹出“系统设置”对话框，在“安全”选项卡下设置文件的传输安全级别为中。即单击选中“安全级－中”单选按钮。



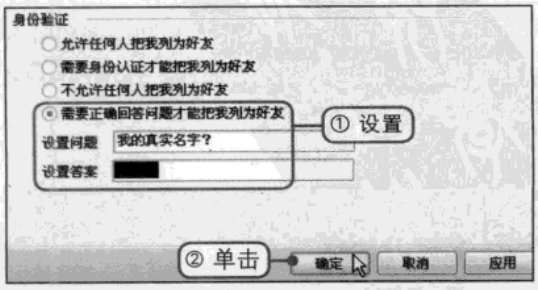
⑤ 设置隐私保护

①单击“隐私保护”选项切换至该选项卡。②分别勾选“只能通过账号或昵称找到我”和“不接收任何陌生人的消息”复选框。



⑥ 设置身份验证

①在“身份验证”选项组中单击选中“需要正确回答问题才能把我列为好友”单选按钮并设置问题和答案。②单击“确定”按钮即可完成设置。

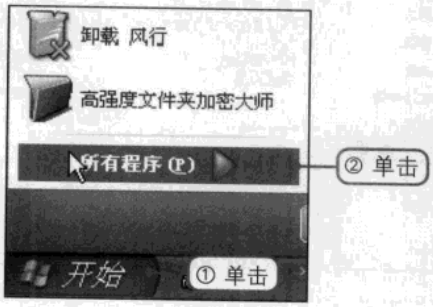


5.3.2 MSN隐私保护

MSN是微软公司推出的一个即时通信软件，全称是Microsoft Service Network，即微软网络服务。由于该软件是用于通信的，因此也要注意隐私的保护。

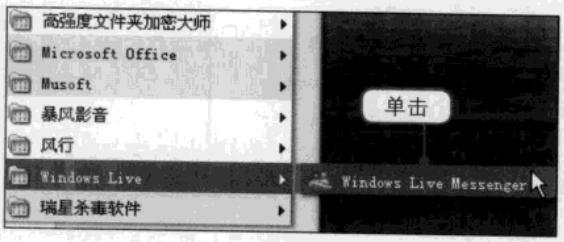
① 单击“所有程序”命令

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“所有程序”命令。



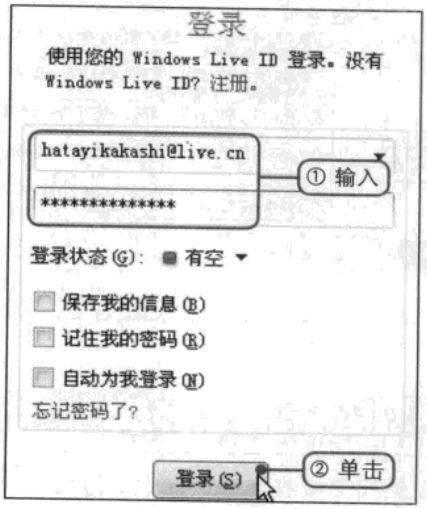
② 启动MSN

在右侧弹出的菜单中单击“Windows Live>Windows Live Messenger”命令。



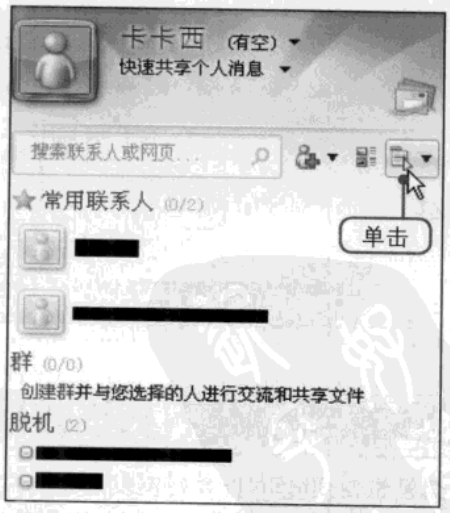
③ 登录MSN

打开Windows Live Messenger登录界面，①在文本框中输入有效的用户名和密码。②单击“登录”按钮。



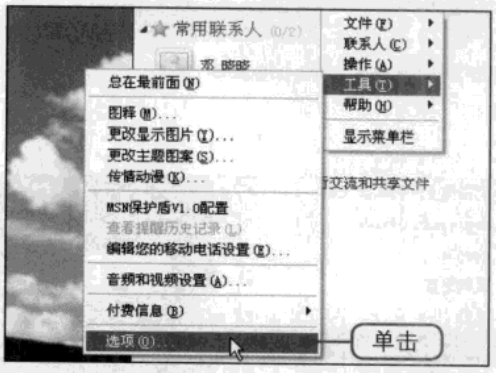
④ 单击“显示菜单”按钮

登录成功之后，在登录界面中单击右侧的 ▾ 按钮。



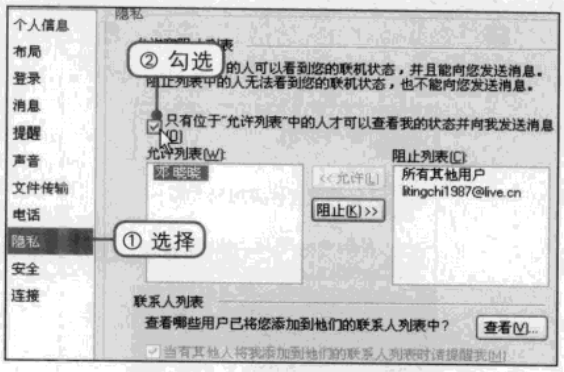
⑤ 打开“选项”对话框

在弹出的菜单中单击“工具>选项”命令，打开“选项”对话框。



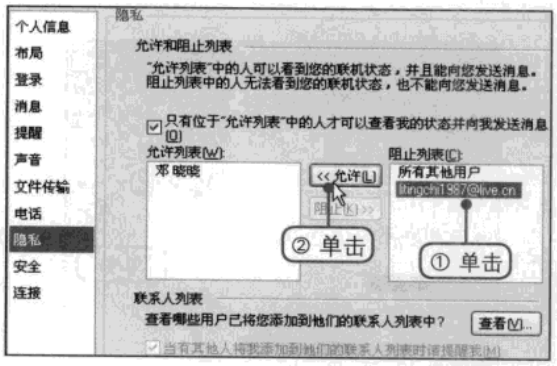
⑥ 隐私保护设置

①在“选项”对话框左侧列表框中选择“隐私”选项切换至该选项卡。②在右侧勾选“只有位于‘允许列表’中的人才可以查看我的状态并向我发送消息”复选框。



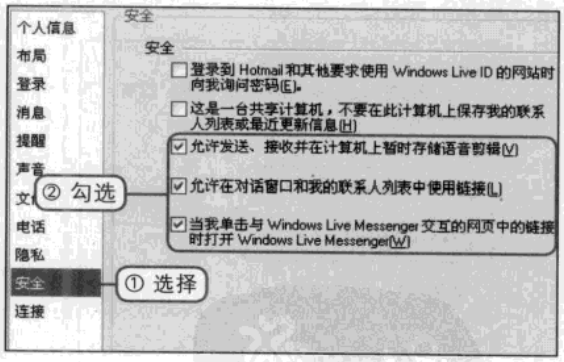
⑦ 将好友添加至允许列表中

①在“阻止列表”列表框中单击选中用户名。②单击左侧的“允许”按钮，则可将好友添加至“允许列表”列表框中。



⑧ 安全设置

①在“选项”对话框左侧列表框中选择“安全”选项切换至该选项卡。②在右侧勾选如下图所示的3个复选框。

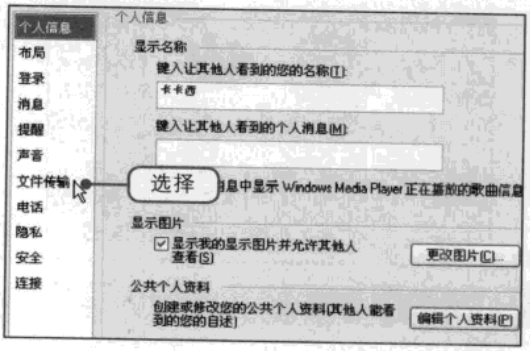


5.3.3 MSN扫描接收文件

如果想使用MSN接收好友发送来的文件，则需要设置扫描接收文件，在设置过程中可使用MSN保护盾扫描，也可使用电脑中的杀毒软件进行扫描。

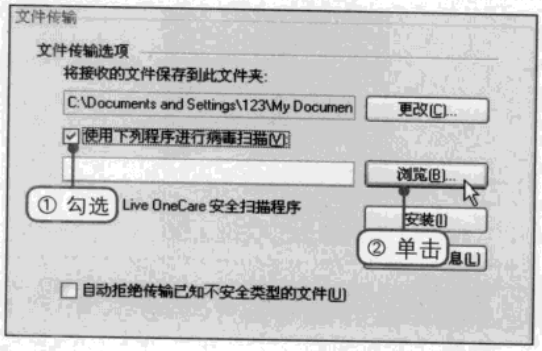
① 切换至“文件传输”选项卡

按照前面的方法打开“选项”对话框，在对话框左侧的列表框中选择“文件传输”选项切换至该选项卡。



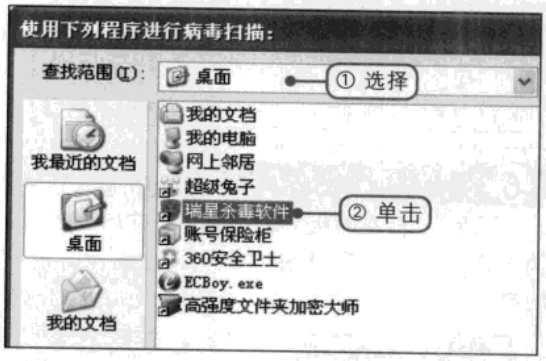
② 设置病毒扫描

①在“选项”对话框右侧勾选“使用下列程序进行病毒扫描”复选框。②单击“浏览”按钮。



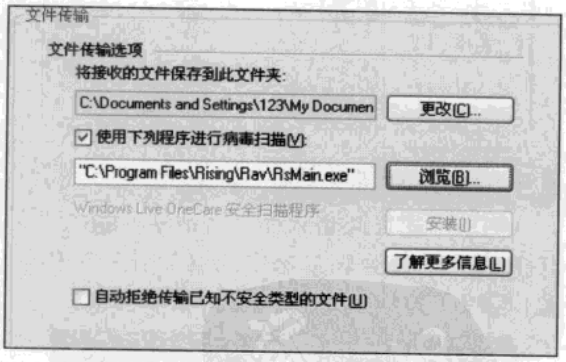
③ 选择病毒扫描的程序

弹出“使用下列程序进行病毒扫描”对话框，①在“查找范围”下拉列表中选择病毒扫描程序所在的位置。②在下方的列表框中单击病毒扫描程序，例如单击选中“瑞星杀毒软件”选项。



④ 保存设置

单击“打开”按钮返回“选项”对话框，用户可在“使用下列程序进行病毒扫描”选项下看见病毒扫描的程序。确认无误后单击“确定”按钮保存退出即可。



5.3.4 安全使用迅雷下载文件

迅雷是一款比较实用的下载软件。由于互联网中的资源并不是全部都是安全的，例如有些资源携带了病毒或者木马，因此在使用迅雷软件下载资源之前需要将其进行安全设置，及时用杀毒软件扫描下载的资源。

① 启动迅雷

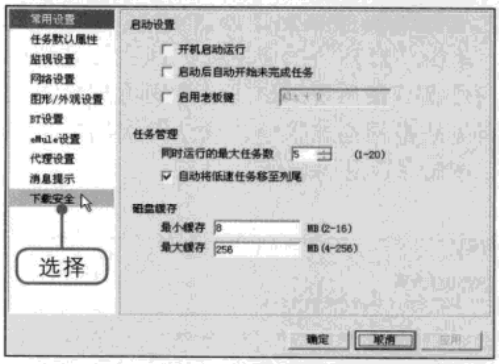
下载并安装好迅雷软件之后会在桌面出现对应的快捷图标，例如迅雷5，双击该图标，启动该应用程序。

② 单击“配置”按钮

打开迅雷5主界面窗口，在窗口中单击“配置”按钮。

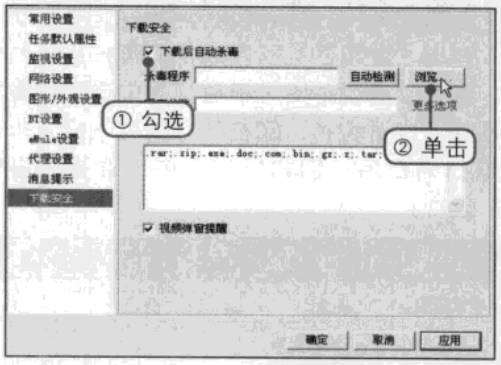
③ 切换至“下载安全”选项卡

打开“配置面板”对话框，在左侧列表框中选择“下载安全”选项。



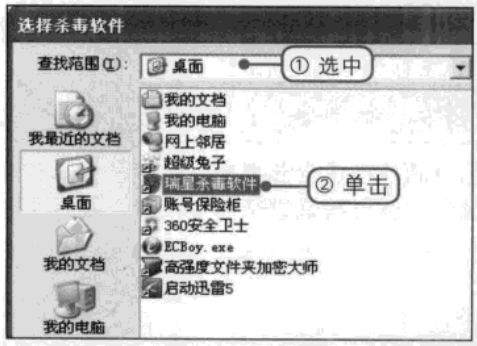
④ 设置下载安全

①在对话框右侧勾选“下载后自动杀毒”复选框。②单击“浏览”按钮。



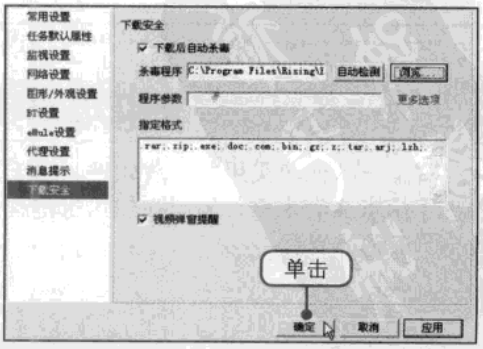
⑤ 选择杀毒软件

弹出“选择杀毒软件”对话框，①在“查找范围”下拉列表中选中杀毒软件所在的位置，②在下方列表框中单击选中杀毒软件。



⑥ 确认选择的杀毒软件

返回“配置面板”对话框中，确认所选择的杀毒软件无误后单击“确定”按钮保存退出即可。

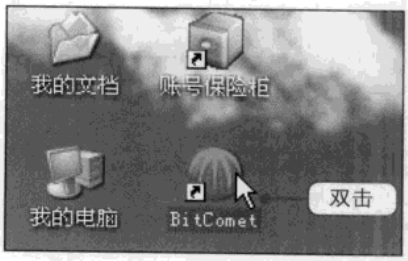


5.3.5 安全使用BitComet下载文件

BitComet是一款强大的下载软件，它不仅能下载资源，而且也能将本地资源上传到互联网中。为使下载的资源安全，使用该软件进行下载之前同样也需要使用杀毒软件扫描。

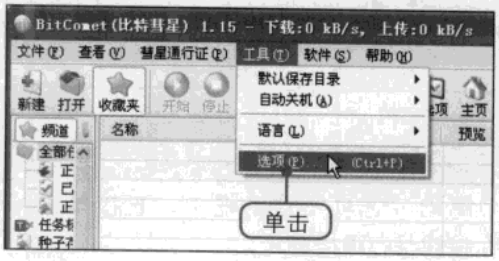
① 启动BitComet

下载并安装好BitComet软件后会在桌面上出现对应的快捷图标，双击该图标，启动该应用程序。



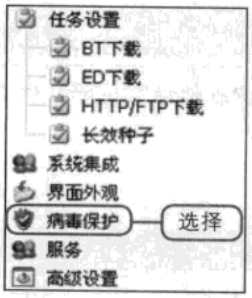
② 单击“选项”命令

打开BitComet的主界面窗口，①在窗口菜单栏中单击“工具>选项”命令。



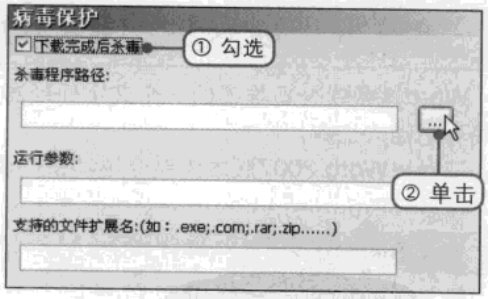
③ 切换至“病毒保护”选项卡

打开“选项”对话框，在左侧列表框中选择“病毒保护”选项切换至该选项卡。



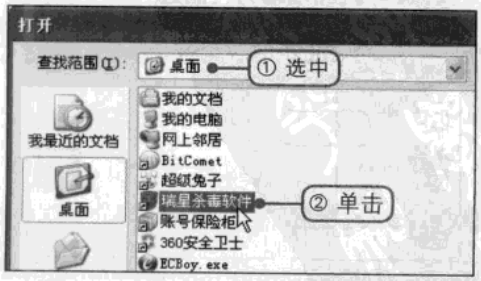
④ 设置病毒保护

①在对话框右侧勾选“下载完成后杀毒”复选框。②单击“杀毒程序路径”文本框右侧的[...]按钮。



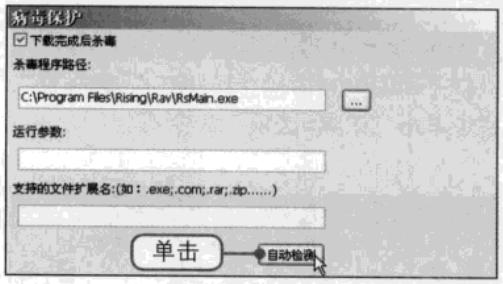
⑤ 选择杀毒软件

弹出“打开”对话框，①在“查找范围”下拉列表中选中杀毒软件所在的位置，②在列表框中单击选中杀毒软件。



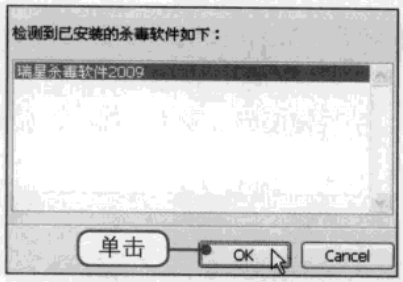
⑥ 单击“自动检测”按钮

单击“打开”按钮后返回“选项”对话框，在对话框右侧单击“自动检测”按钮，弹出“检测提示”对话框。



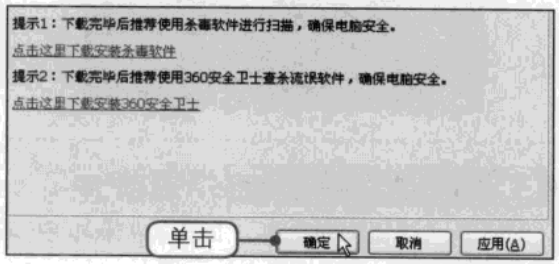
⑦ 单击OK按钮

在“检测提示”对话框中显示了电脑中的杀毒软件，直接单击OK按钮。



⑧ 保存设置

返回“选项”对话框中，直接单击“确定”按钮保存退出即可。



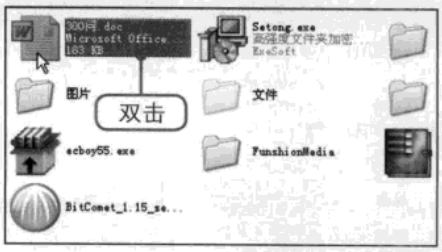
5.3.6 设置Word密码

Word是微软公司推出的一个文字处理器应用程序，在使用该软件编写重要文件之后为其设置密码可防他人盗取。

下面以Word 2007版本为例介绍其密码设置的方法。

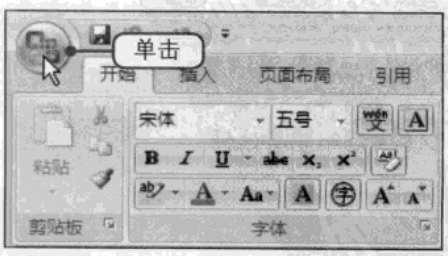
① 打开Word文档

打开Word文档所在的磁盘窗口，双击Word文档，例如双击“300问”文档。



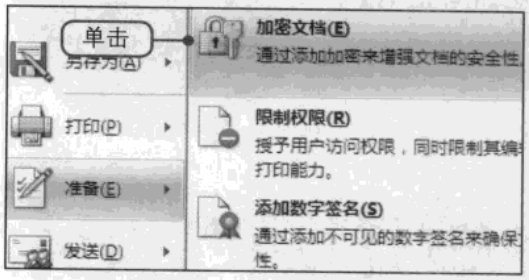
② 单击“文件”按钮

打开Word文档，单击文档左上角的“文件”按钮。



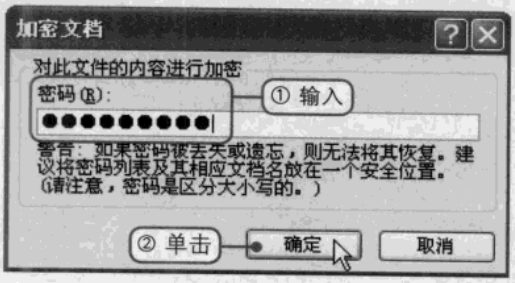
③ 单击“加密文档”命令

在弹出的菜单中单击“准备>加密文档”命令。



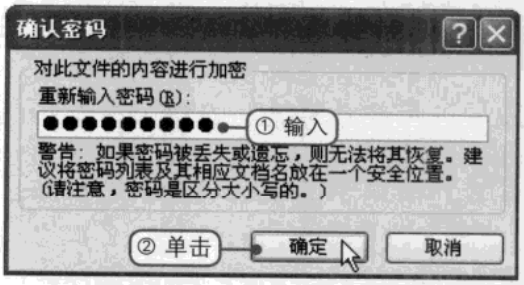
④ 设置密码

弹出“加密文档”对话框，①在“密码”文本框中输入设置的密码。②单击“确定”按钮。



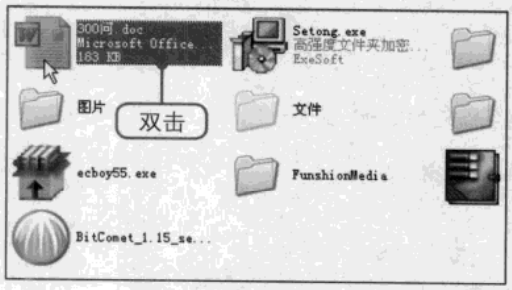
⑤ 再次输入密码

弹出“确认密码”对话框，①在“重新输入密码”文本框中输入密码。②单击“确定”按钮。



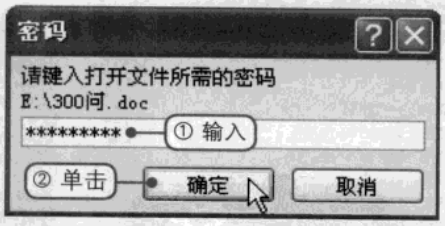
⑥ 打开加密的文档

返回步骤1中的窗口，在窗口中双击打开加密的Word文档。



⑦ 加密成功

弹出“密码”对话框，要求键入打开文档所需的密码，①在文本框中输入正确的密码，②单击“确定”按钮即可打开Word文档。



为Excel设置密码

Excel是微软办公套装软件的一个重要组成部分，可以进行各种数据的处理、统计分析和辅助决策操作。Excel软件被广泛地应用于管理、统计、财经、金融等众多领域。若需要对重要的Excel文档进行加密，可以在打开需要设置密码的Excel文档后，按照设置Word密码的方法为Excel设置密码。

Chapter 06

系统与重要数据的备份与还原

对电脑中的系统和重要数据做好了安全设置也不可大意，为了防止意外发生，用户需要对系统和电脑中的重要数据进行备份。可使用GHOST和一键还原精灵对系统进行备份。使用相应的备份工具对电脑中的驱动程序、重要邮件、QQ聊天信息等重要数据进行备份。一旦发生异常，则直接将备份文件还原即可，避免遭受重大的损失。

重点知识

1. 使用系统还原工具备份与还原系统
2. 使用一键GHOST备份与还原系统
3. 使用一键还原精灵备份与还原系统
4. 备份与还原Outlook Express邮件
5. 使用驱动精灵备份与还原驱动程序
6. 使用系统备份工具备份与还原注册表
7. 备份与还原“IE收藏夹”
8. 备份与还原QQ聊天记录
9. 重要数据刻录保护

视频文件

参见随书光盘：视频教程\Chapter 06

Chapter 06 系统与重要数据的备份与还原

- 6.1.1 创建还原点
- 6.1.2 还原系统
- 6.1.3 撤销上一次还原
- 6.2.1 使用一键GHOST备份系统
- 6.2.2 使用一键GHOST还原系统
- 6.3.1 设置启动菜单
- 6.3.2 使用一键还原精灵备份系统
- 6.3.3 使用一键还原精灵还原系统
- 6.4.1 使用驱动精灵备份驱动程序
- 6.4.2 使用驱动精灵还原驱动程序
- 6.5.1 在注册表编辑器中备份注册表
- 6.5.2 在注册表编辑器中还原注册表
- 6.6.1 备份Outlook Express邮件
- 6.6.2 还原Outlook Express邮件
- 6.7.1 备份“IE收藏夹”
- 6.7.2 还原“IE收藏夹”
- 6.8.1 备份QQ聊天记录
- 6.8.2 还原QQ聊天记录
- 6.9 重要数据刻录保护

6.1 使用系统还原工具备份与还原系统

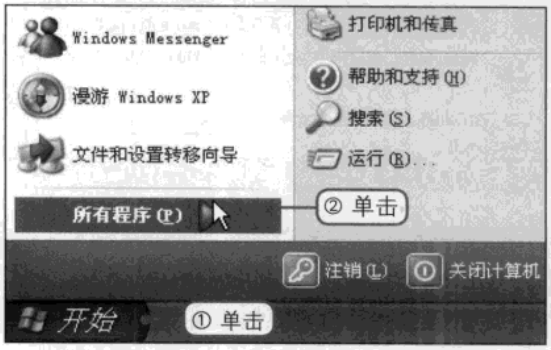
Windows XP操作系统自带的系统还原工具可供用户备份系统，即创建还原点，使用该工具备份系统可创建不同的还原点，当系统发生异常时用户可选择不同的还原点进行还原，若还原错误也可撤销还原再次选择。

6.1.1 创建还原点

系统还原服务会自动建立一个非常易于辨认的还原点，用户可利用此还原点将系统还原到先前的状态，也可自行创建还原点。

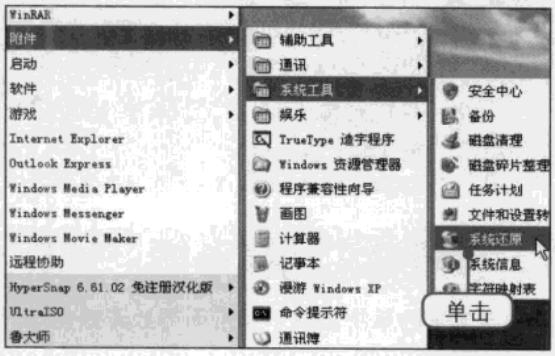
① 单击“所有程序”命令

①在桌面上单击“开始”按钮。②弹出“开始”菜单，在菜单中单击“所有程序”命令。



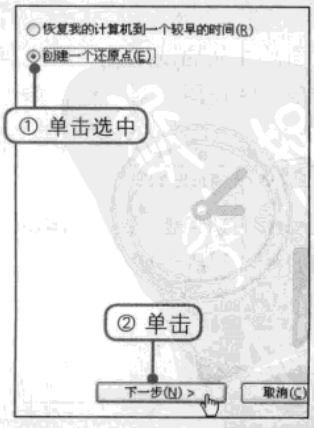
② 启动系统还原应用程序

在右侧弹出的菜单中单击“附件>系统工具>系统还原”命令，启动系统还原应用程序。



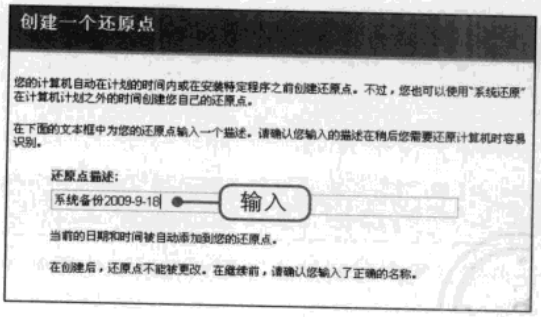
③ 创建还原点

打开“欢迎使用系统还原”对话框，①在对话框右侧单击选中“创建一个还原点”单选按钮。②单击“下一步”按钮。



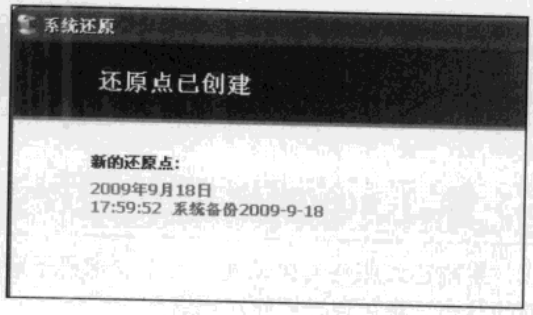
④ 还原点描述

打开“创建一个还原点”对话框，在“还原点描述”文本框中输入还原点名称，接着单击“创建”按钮。



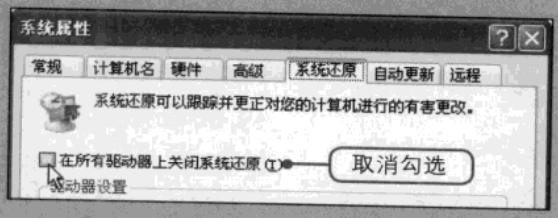
⑤ 创建成功

打开“还原点已创建”对话框，显示了创建还原点的详细信息，直接单击“关闭”按钮退出即可。



开启系统还原功能

若用户需要使用系统还原工具来还原系统，则首先需右击“我的电脑”图标，在弹出的快捷菜单中单击“属性”命令，打开“系统属性”对话框，在“系统还原”选项卡下取消勾选如右图所示的复选框。

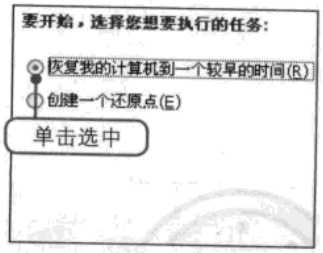


6.1.2 还原系统

当电脑的系统出现了异常而导致无法启动时，可通过系统还原工具将系统直接还原。

① 选择系统还原

按照前面的方法启动系统还原应用程序，打开“欢迎使用系统还原”对话框，单击选中“恢复我的计算机到一个较早的时间”单选按钮。

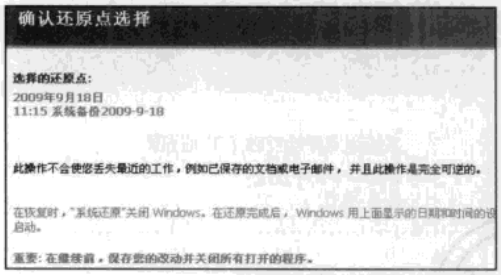


② 选择创建的还原点

单击“下一步”按钮打开“选择一个还原点”对话框，选择需要还原的还原点后单击“下一步”按钮。

③ 确认选择的还原点

打开“确认还原点选择”对话框，确认选择的还原点无误后单击“下一步”按钮。

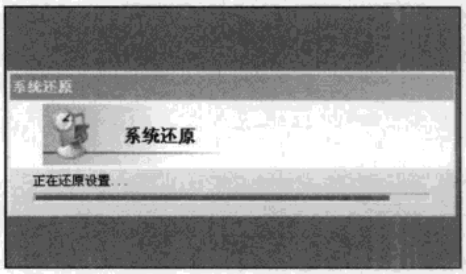


④ 关闭计算机

当用户执行了还原操作之后，计算机自动进入关闭界面。

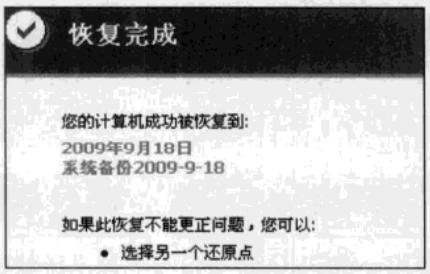
⑤ 还原设置

同时弹出“系统还原”对话框，在对话框中显示了正在还原设置的进度。



⑥ 还原成功

还原设置完成后系统会按照还原的时间和日期来重启计算机，并在打开的“恢复完成”对话框中显示恢复完成。

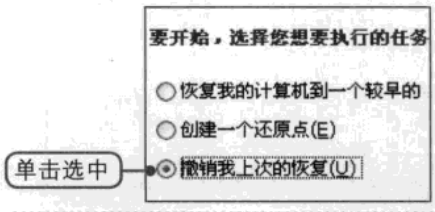


6.1.3 撤销上一次还原

若还原系统后发现在还原系统的操作过程中所选择的还原点错误后，可执行撤销上一次还原的操作，使系统恢复到还原前的状态，接着再次还原系统。

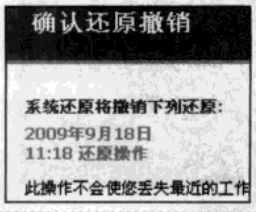
① 撤销上次的恢复

按照前面的方法打开系统还原应用程序，在右侧单击选中“撤销我上次的恢复”单选按钮，接着单击“下一步”按钮。



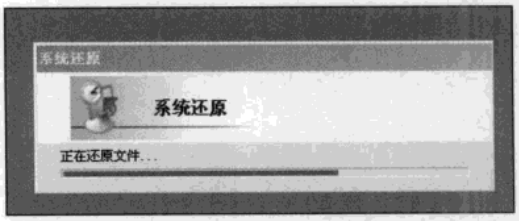
② 确认还原撤销

打开“确认还原撤销”对话框，在对话框中列出了选择撤销还原点的日期和名称，确认后单击“下一步”按钮重启计算机。



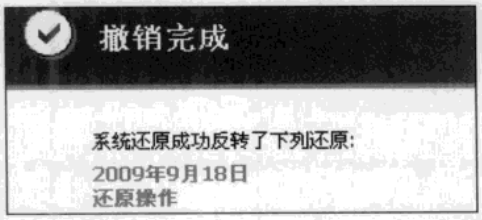
③ 查看撤销的进度

重启过程中弹出“系统还原”对话框，可以看见撤销还原的进度，请耐心等待。



④ 撤销完成

重启后弹出“撤销完成”对话框，单击“确定”按钮后关闭对话框即可。



6.2 使用一键GHOST备份与还原系统

一键GHOST与Ghost都是实现备份和还原功能的软件。一键GHOST操作简单，只需按一个键就能实现全自动无人值守操作，适合初学者使用；而Ghost除了有一键GHOST的全部功能外还外加了如-rb、-fx、-sure等很多命令和参数，没有一定电脑基础的人操作起来有一定的困难，而且风险也很大。本节主要介绍使用一键GHOST进行系统备份与还原的方法。

6.2.1 使用一键GHOST备份系统

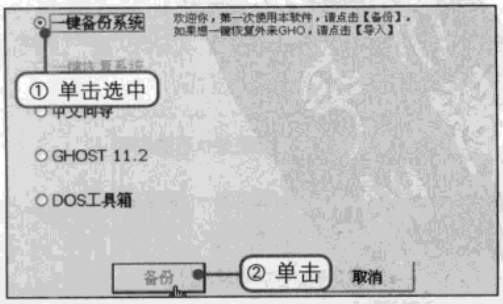
使用一键GHOST备份与还原系统就是将磁盘分区的物理信息备份为一个镜像文件，通过还原操作将系统恢复到备份时的正常状态。在使用该软件前需要在网络上下载并将其安装至计算机中，然后便可使用它来备份当前系统。

① 启动一键GHOST

用户下载并安装一键GHOST后会在桌面上出现对应的快捷图标，双击“一键GHOST”快捷图标，启动该软件。

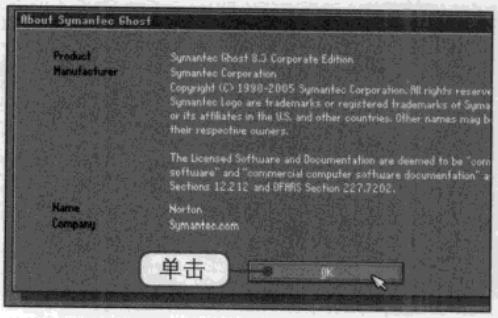
② 单击“备份”按钮

打开一键GHOST主界面窗口，①单击选中“一键备份系统”单选按钮。②单击“备份”按钮，电脑自动重启。



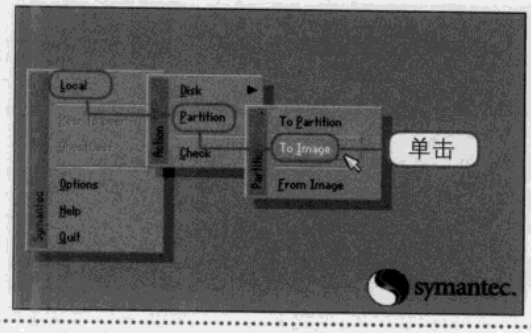
③ 提示界面

电脑重启后会弹出提示对话框，直接单击OK按钮打开一键GHOST的主菜单窗口。



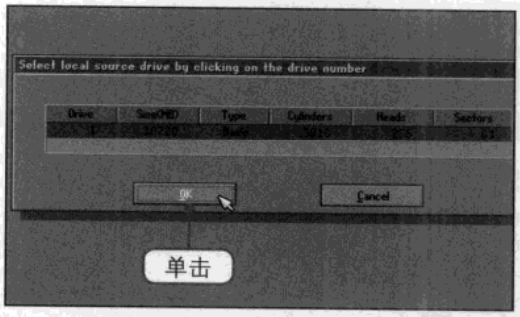
④ 选择备份

在GHOST主菜单窗口中单击“Local>Partition>To Image”命令。



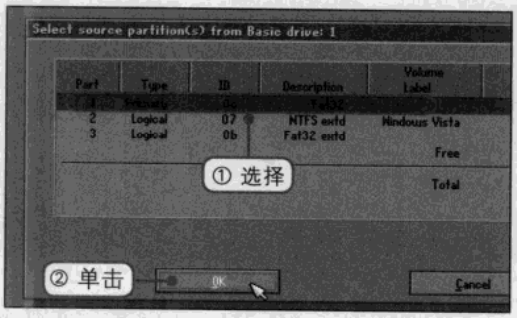
⑤ 选择硬盘

一键GHOST软件要求用户选择硬盘，由于该电脑中只有一个硬盘，因此直接单击OK按钮即可。



⑥ 选择备份的分区

在打开的列表框中显示了电脑的所有分区。①通过方向键选择安装系统的分区，例如选中C盘分区。②单击OK按钮。



⑦ 设置备份的镜像文件

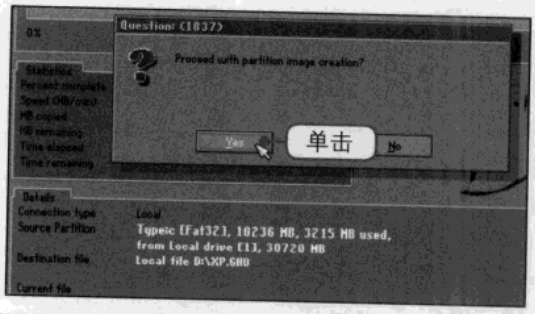
①在Look in下拉列表中选择保存文件的路径。②在File name文本框中输入文件名称。③单击Save按钮。

⑧ 选择压缩文件的方式

弹出提示框，其中No指不压缩文件，Fast指压缩比例小速度快，High指压缩比例大速度慢，单击Fast按钮。

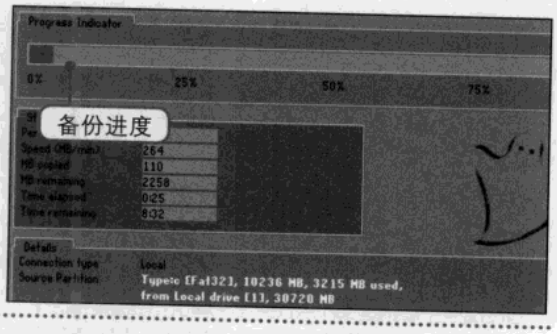
⑨ 确认备份

再次弹出提示框，提示用户是否确认备份，单击Yes按钮确认备份。



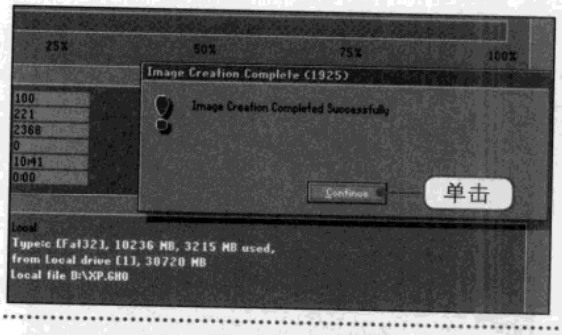
⑩ 查看备份进度

此时可在界面中看见备份的进度，只需耐心等待即可。



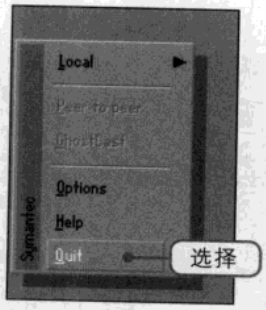
⑪ 备份完成

当进度条到达100%时会弹出一个备份完成的提示框，单击Continue按钮。



⑫ 退出一键GHOST

此时界面返回一键GHOST主菜单窗口，直接选择Quit选项退出即可。

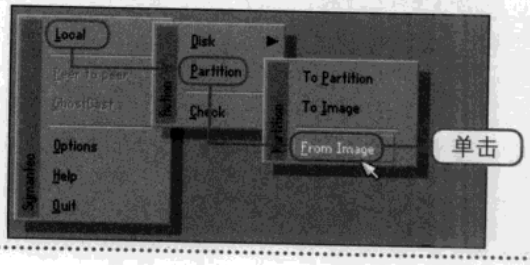


6.2.2 使用一键GHOST还原系统

当系统出现异常时用户可在启动管理界面中选择启动一键GHOST，然后按照下面的操作完成系统还原操作。

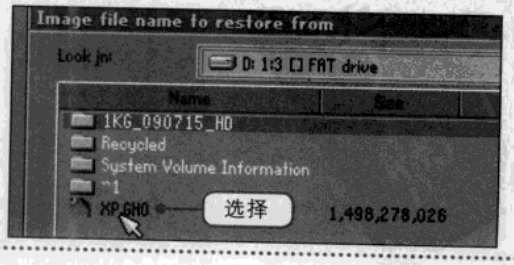
① 选择读取镜像文件

按照前面的方法打开GHOST主菜单窗口，然后单击“Local>Partition>From Image”命令。



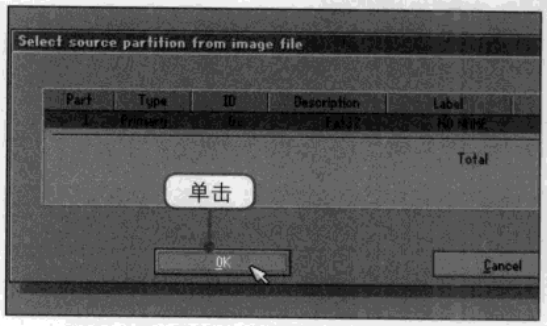
② 选择备份文件

在Look in下拉列表中选择文件所在的分区并选中文件，然后单击Open按钮。



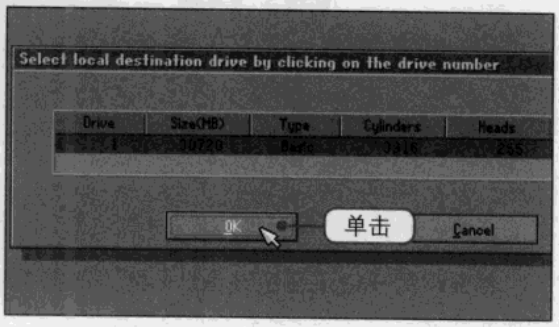
③ 核对镜像文件信息

在打开的界面中核对镜像文件的相关信息，确认无误后单击OK按钮。



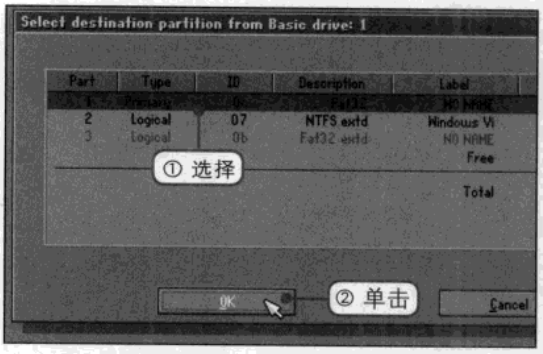
④ 选择硬盘

打开选择硬盘的界面，由于该计算机中只有一个硬盘，因此直接单击OK按钮即可。



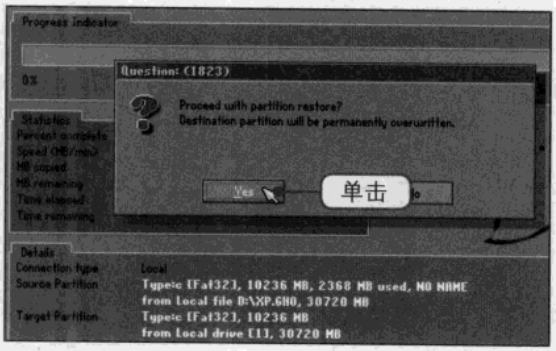
⑤ 选择需要恢复的系统分区

打开新的界面，①单击选中系统所在的分区，这里选择“1”选项。②单击下方的OK按钮。



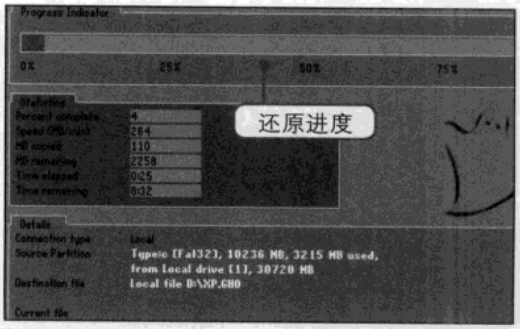
⑥ 确认选择

弹出提示框，提示用户是否确认所选择的恢复分区，确认无误后单击Yes按钮。



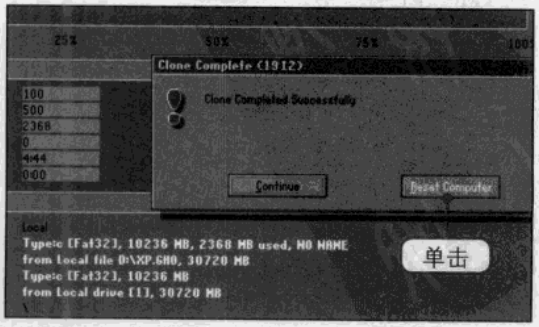
⑦ 开始还原

此时可在界面中看见GHOST还原系统的进度，请耐心等待。



⑧ 重启电脑

当进度条到达100%时，弹出还原成功的提示框，直接单击Reset Computer按钮重新启动电脑即可还原成功。



6.3 使用一键还原精灵备份与还原系统

一键还原精灵是一款“傻瓜式”的系统备份和还原工具，它具有安全、稳定、快速和绝不破坏硬盘数据的特点。用户可使用一键还原精灵对系统分区备份，当系统出现异常时可将系统还原至备份时的状态。没有软驱或光驱的电脑同样可以安装该软件。

6.3.1 设置启动菜单

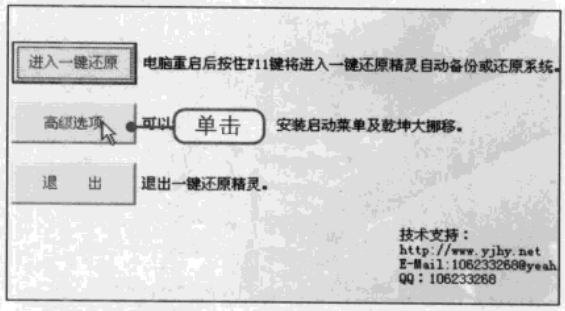
若要使用一键还原精灵备份系统，则需要首先安装并设置启动菜单，否则用户在每次开机后都需要快速地按下F11键来启动该软件。

① 启动一键还原精灵

双击桌面上的“一键还原精灵装机版”快捷图标，启动该应用软件。

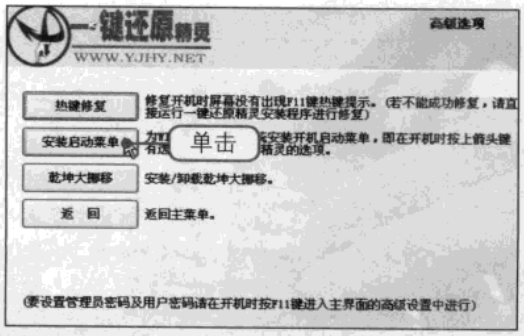
② 单击“高级选项”按钮

打开一键还原精灵主界面窗口，在窗口的左侧单击“高级选项”按钮。



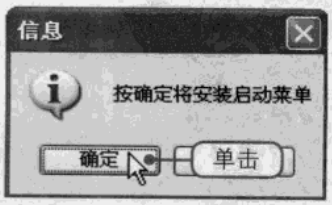
③ 单击“安装启动菜单”按钮

打开新的界面，单击“安装启动菜单”按钮。



④ 确认安装

弹出“信息”提示框，提示用户按确定将安装启动菜单，单击“确定”按钮。

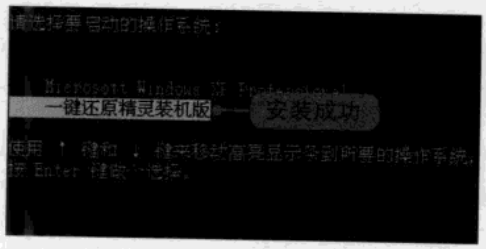


⑤ 安装完毕

等待片刻后弹出“信息”提示框，提示用户安装完毕，单击“确定”按钮并重新启动电脑。

⑥ 安装成功

重启后打开如下界面，在“请选择要启动的操作系统”选项组中可以看见“一键还原精灵装机版”选项，即安装成功。

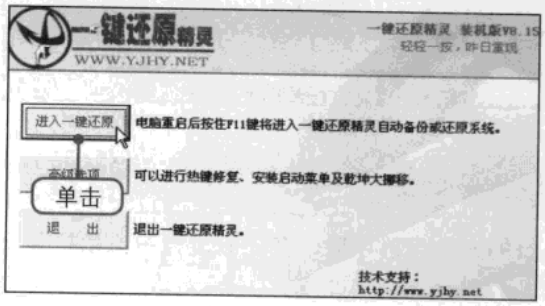


6.3.2 使用一键还原精灵备份系统

设置好启动菜单之后，就可以在启动管理器界面下启动一键还原精灵来备份系统了。

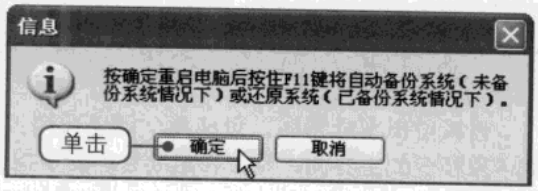
① 单击“进入一键还原”按钮

双击桌面上的快捷图标打开一键还原精灵主界面窗口，在窗口中单击“进入一键还原”按钮。



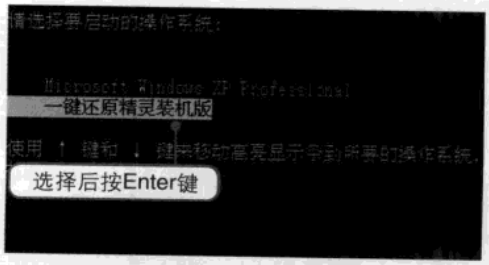
② 重新启动电脑

弹出“信息”提示框，提示用户重新启动电脑后按下F11键将自动备份系统或还原系统，单击“确定”按钮。



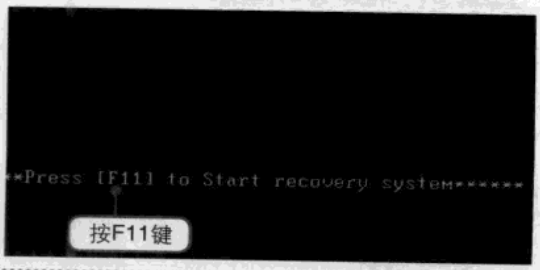
③ 选中一键还原精灵

重启电脑后打开如下图所示的界面，通过方向键选择“一键还原精灵装机版”选项并按 Enter 键。



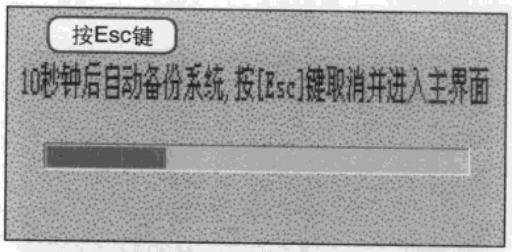
④ 按F11键

此时屏幕会出现Press [F11] to Start recovery system字幕，直接按F11键。



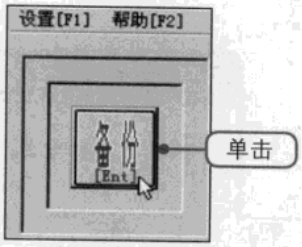
⑤ 进入一键还原精灵主界面

打开如下所示的界面，按下Esc键进入一键还原精灵主界面。



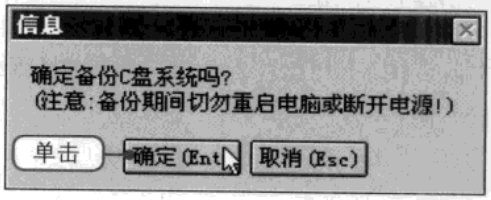
⑥ 单击“备份”按钮

在打开的主界面中单击“备份”按钮开始备份系统。



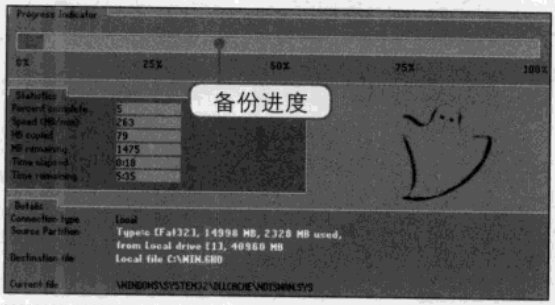
⑦ 确认备份

弹出“信息”提示框，提示用户是否确认备份C盘系统，直接单击“确定”按钮。



⑧ 开始备份

此时在界面中可以看见备份的进度，请耐心等待，完成后计算机自动重启，即备份完成。

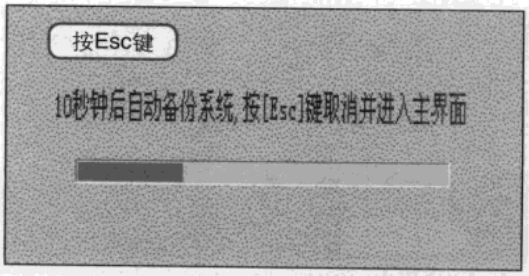


6.3.3 使用一键还原精灵还原系统

当系统出现异常时，可使用一键还原精灵将备份的文件直接还原，在还原过程中不用打开一键还原精灵的主界面，直接在启动管理器中操作即可。

① 进入一键还原精灵主界面

按照前面的方法打开如下界面，按下Esc键进入一键还原精灵主界面。

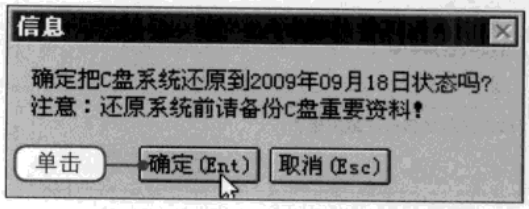


② 单击“还原”按钮

在打开的主界面中单击“还原”按钮开始将备份文件还原。

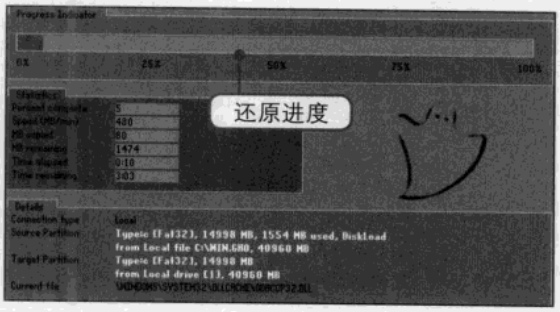
③ 确认还原

弹出“信息”提示框，提示用户是否确认把C盘系统还原，直接单击“确定”按钮确定还原。



④ 开始还原

此时在界面中可以看见还原系统的进度，只需耐心等待即可，完成后计算机自动重启进入系统备份时的状态。



6.4 使用驱动精灵备份与还原驱动程序

驱动精灵是一款集驱动程序和硬件检测为一体的专业级驱动管理和维护工具，该软件为用户提供了驱动备份、恢复、安装、删除、在线更新等比较实用的功能。一般情况下用户重新安装操作系统后都需要手动安装驱动程序，使用驱动精灵可以在重新安装系统前将驱动程序备份，操作系统安装完成后将驱动程序还原即可。

6.4.1 使用驱动精灵备份驱动程序

可登录驱动之家网站（http://www.mydrivers.com）下载驱动精灵软件，下载后将其安装到电脑中，接着就可使用该软件备份电脑中的驱动程序了。在备份驱动程序之前，用户可以将驱动程序升级至最新版本。

① 启动驱动精灵

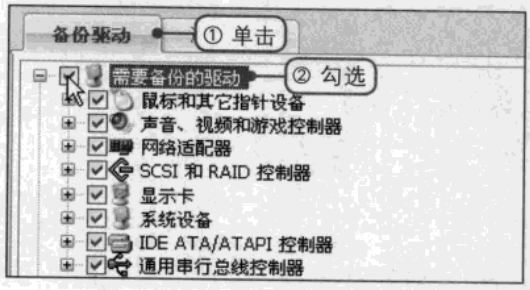
下载并安装好驱动精灵之后会在桌面上出现对应的快捷图标，双击该图标，启动驱动精灵。

② 单击“备份还原”按钮

打开驱动精灵主界面窗口，单击“备份还原”按钮。

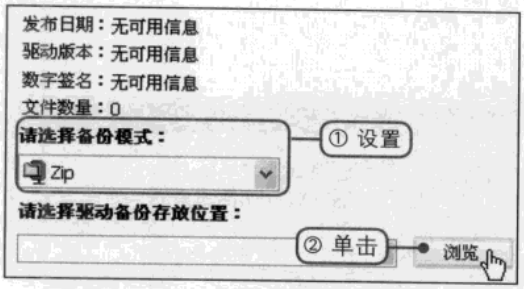
3 选择需要备份的驱动程序

①在“备份还原”界面中单击“备份驱动”标签切换至该选项卡。②勾选“需要备份的驱动”复选框。



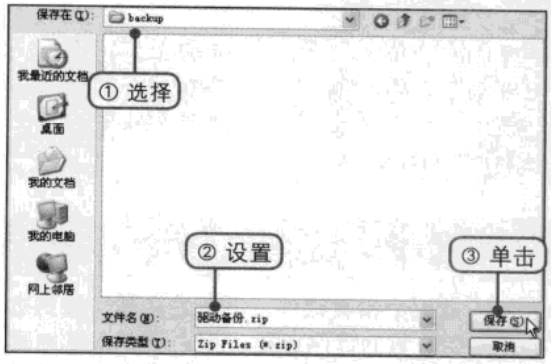
4 设置备份模式

①在窗口的右侧设置备份模式为Zip。②单击“请选择驱动备份存放位置”下拉列表框右侧的“浏览”按钮。



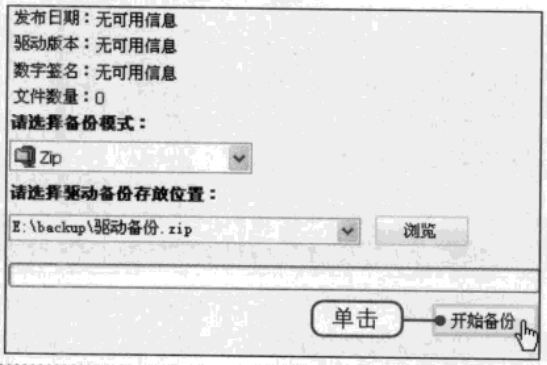
5 设置保存选项

弹出Save As对话框，①在“保存在”下拉列表中选择保存位置。②设置保存的文件名。③单击“保存”按钮。



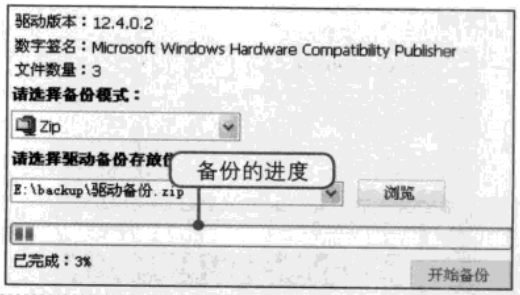
6 开始备份

返回驱动精灵主界面窗口，单击窗口右下方的“开始备份”按钮开始备份。



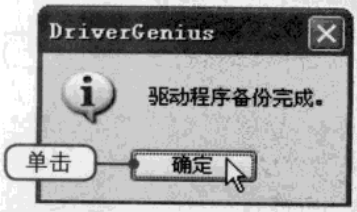
7 查看备份的进度

此时可在窗口右下方看见备份的进度，请耐心等待。



8 备份成功

完成后弹出DriverGenius提示框，提示用户驱动程序备份完成。单击“确定”按钮。



6.4.2 使用驱动精灵还原驱动程序

用户备份的驱动程序文件放在除系统分区之外的其他分区中，当用户重装系统或者发生驱动程序出现问题时，可直接使用该软件将备份文件还原。

① 单击“备份还原”按钮

按照前面的方法打开驱动精灵主界面窗口，在窗口中单击“备份还原”按钮。

② 选择需要恢复的驱动程序

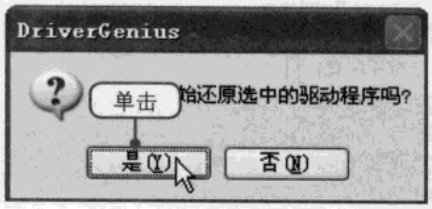
①单击“还原驱动”标签切换至该选项卡。②勾选“驱动备份“复选框。

③ 单击“开始还原”按钮

在主界面窗口的右边单击“开始还原”按钮。

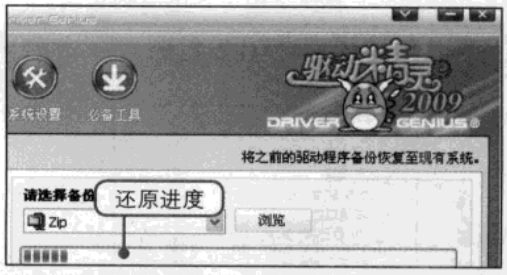
④ 确认还原

弹出DriverGenius提示框，提示用户是否确认还原，直接单击“是”按钮。



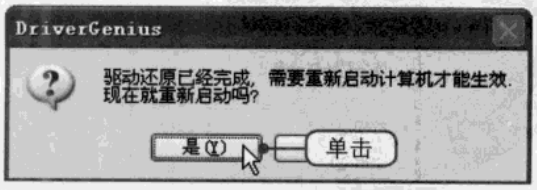
⑤ 查看还原的进度

返回主界面窗口，可在窗口右侧看见还原的进度，请耐心等待。



⑥ 重新启动电脑

完成后弹出DriverGenius提示框，提示用户还原完成，需要重启计算机才能生效，单击“是”按钮重启电脑即可。



6.5 使用系统备份工具备份与还原注册表

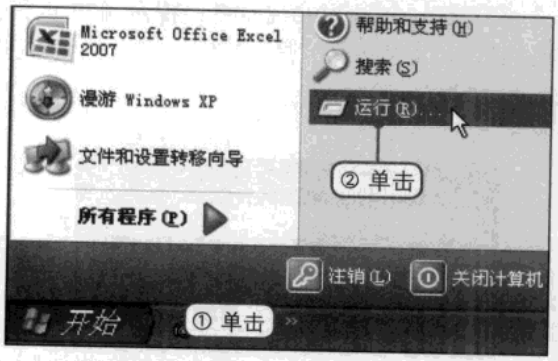
注册表是Windows操作系统的核心，它存储和管理着整个操作系统、应用程序的关键数据。在系统中起着非常重要的作用，用户在日常的工作和学习中应做好注册表的备份工作，当用户操作不当导致注册表出现问题时可直接将备份文件还原。

6.5.1 在注册表编辑器中备份注册表

在注册表编辑器中备份注册表之前需要打开注册表编辑器，然后在打开的窗口中执行导出操作，即可备份注册表。

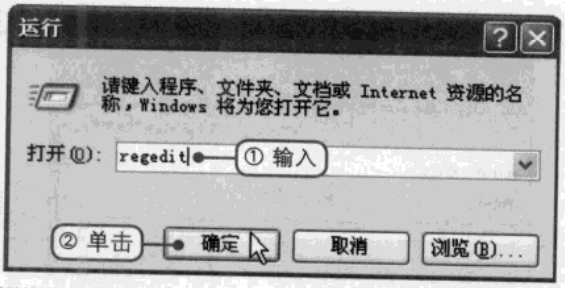
① 打开“运行”对话框

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“运行”命令，打开“运行”对话框。



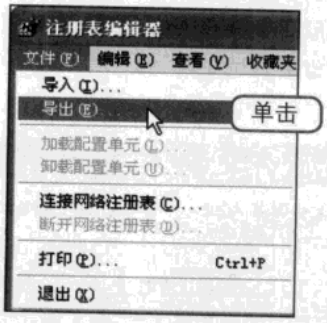
② 输入regedit命令

①在“打开”文本框中输入regedit命令。②单击“确定”按钮，打开“注册表编辑器”窗口。



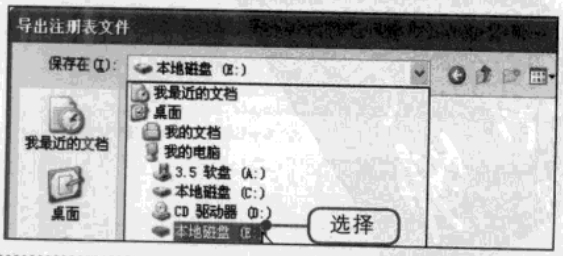
③ 单击“导出”命令

单击菜单栏中的“文件>导出”命令。



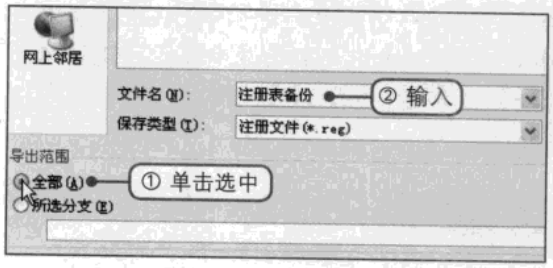
④ 选择注册表备份文件的保存位置

弹出“导出注册表文件”对话框，单击“保存在”下拉列表框右侧的下三角按钮，接着在下拉列表中选择备份文件的保存位置。



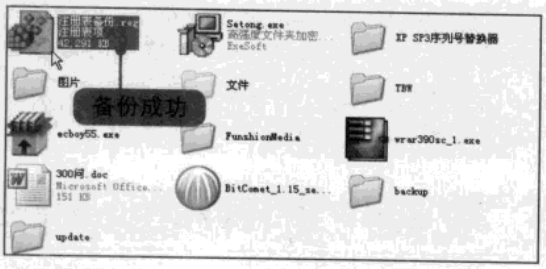
⑤ 设置导出范围和文件名

①在对话框底部的“导出范围”选项组中单击选中“全部”单选按钮。②在“文件名”文本框中输入备份文件的文件名。



⑥ 备份成功

单击“保存”按钮，打开前面设置的保存位置所在的窗口，可在窗口看见注册表的备份文件，即备份成功。

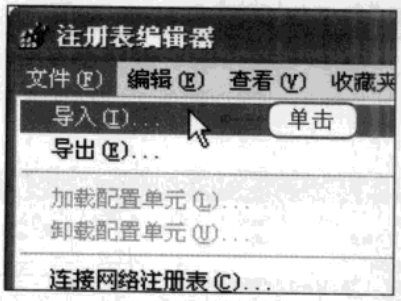


6.5.2 在注册表编辑器中还原注册表

备份的注册表文件建议放置在除系统盘分区之外的其他分区中，当注册表发生故障时可将备份文件导入注册表达到还原的目的。首先要按照上一小节所述的方法打开“注册表编辑器”窗口，然后按以下步骤操作即可还原注册表。

① 单击“导入”命令

按照前面的方法打开“注册表编辑器”窗口，单击菜单栏中的“文件> 导入”命令。打开“导入注册表文件”对话框。



② 导入注册表

在“查找范围”下拉列表中选择备份文件所在的位置并选中备份文件，单击“打开”按钮即可将备份的注册表文件还原。

6.6 备份与还原Outlook Express邮件

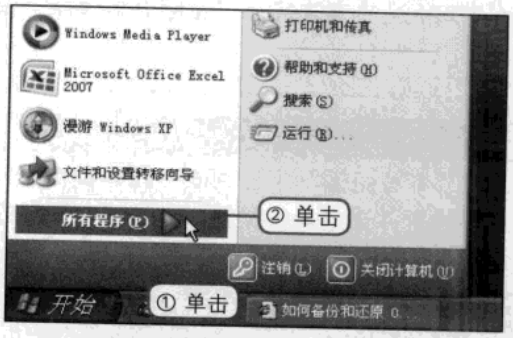
Outlook Express 是 Windows 操作系统自带的一款电子邮件客户端，简称 OE，它在桌面上实现了全球范围的联机通信，在使用 Outlook Express 进行通信时需要定期地对其中的邮件进行备份，当该软件遭到破坏时，可在重新安装该软件后将备份的邮件导入即可将损失减小到最低。

6.6.1 备份Outlook Express邮件

可以使用Outlook Express查找其邮件的存储位置，然后将其全部复制到安全地方即可完成备份。

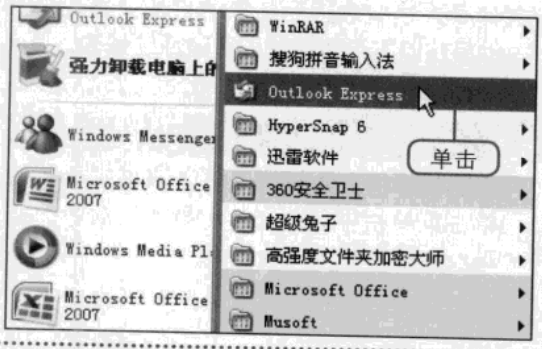
① 单击“所有程序”命令

①单击桌面上的“开始”按钮，弹出“开始”菜单。②在“开始”菜单中单击“所有程序”命令。



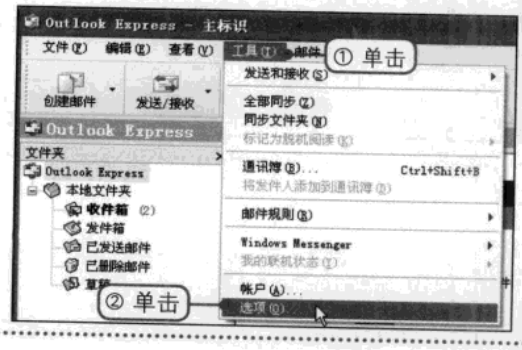
② 启动Outlook Express

在右侧弹出的菜单中单击“Outlook Express”命令，启动Outlook Express软件。



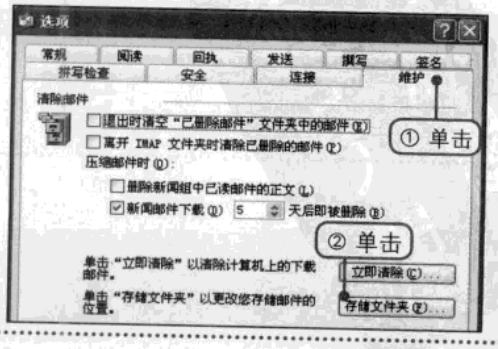
③ 单击“选项”命令

①在Outlook Express主界面窗口的菜单栏中单击“工具”选项。②在弹出的菜单中单击“选项”命令。



④ 单击“存储文件夹”按钮

弹出“选项”对话框，①单击“维护”标签切换至该选项卡下。②单击“存储文件夹”按钮。

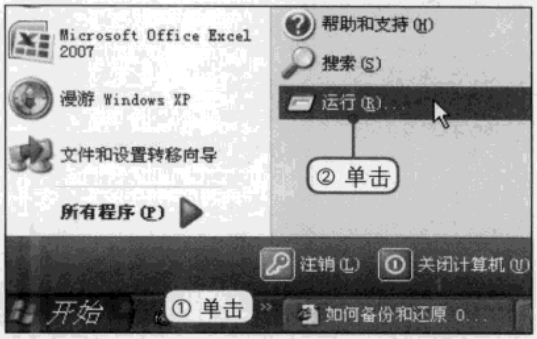


5 复制文件夹地址

弹出“存储位置”对话框，①选中文件夹地址并按Ctrl+C键复制该地址。②单击“确定”按钮关闭对话框。

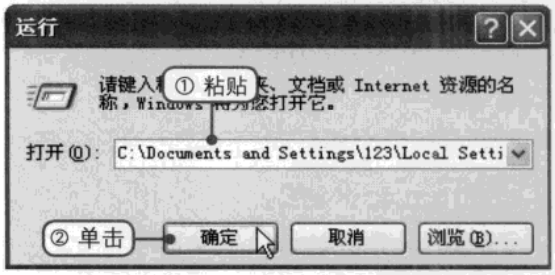
6 打开“运行”对话框

①再次单击桌面上的“开始”按钮，②在弹出的“开始”菜单中单击“运行”命令，打开“运行”对话框。



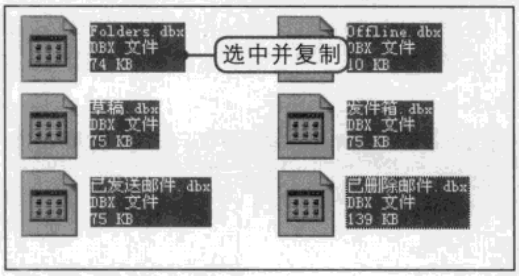
7 打开存储文件夹

①在“打开”文本框中按Ctrl+V键粘贴步骤5中复制的地址。②单击“确定”按钮。



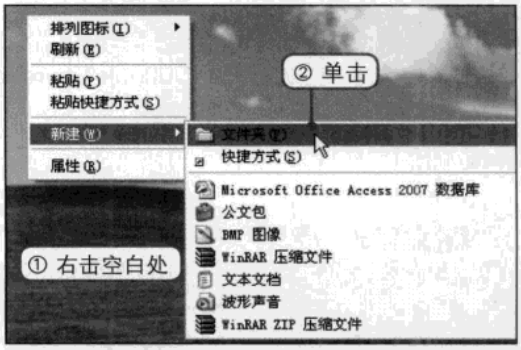
8 复制邮件

打开存储文件夹，按Ctrl+A键选中全部的邮件。接着按Ctrl+C键复制所有的邮件。



9 新建文件夹

返回桌面，①右击桌面上任意空白处。②在弹出的快捷菜单中单击“新建>文件夹”命令。

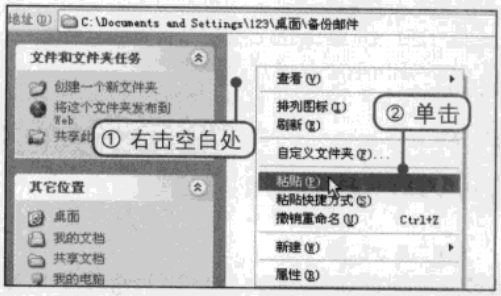


10 重命名文件夹

将该文件夹重命名为“备份邮件”并按Enter键。接着双击该文件夹，打开“备份邮件”窗口。

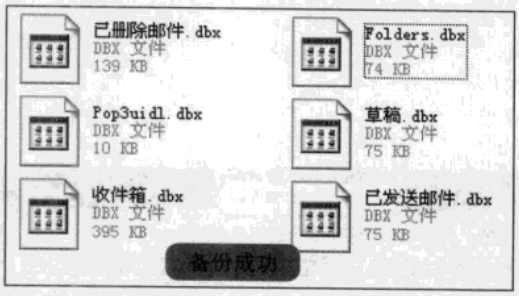
⑪ 单击“粘贴”命令

①右击窗口中的任意空白处。②在弹出快捷菜单中单击“粘贴”命令。



⑫ 备份成功

此时存储文件夹中的所有邮件全部复制到新建的文件夹中，即备份成功。

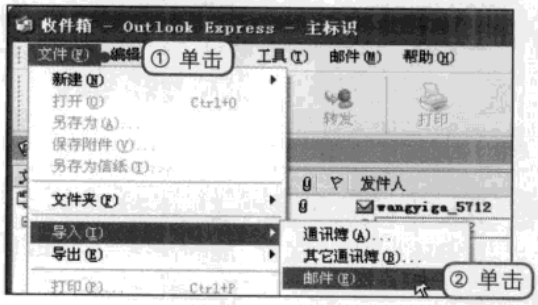


6.6.2 还原Outlook Express邮件

当系统出现异常或者Outlook Express无法使用时，可重新安装该软件，然后将备份的邮件直接导入即可。

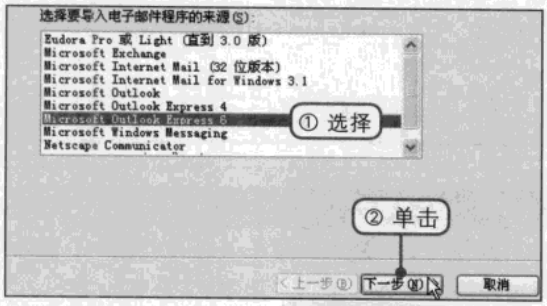
① 单击“邮件”命令

按照前面的方法启动Outlook Express，①单击菜单栏中“文件”选项。②在弹出的菜单中依次单击“导入>邮件”命令。



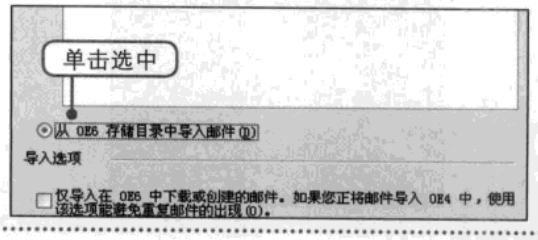
② 选择电子邮件的来源

打开“Outlook Express导入”对话框，①在列表框中选中“Microsoft Outlook Express 6”选项。②单击“下一步”按钮。



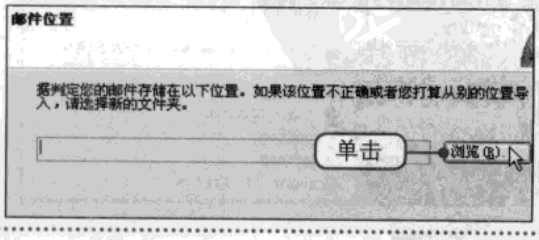
③ 从OE6存储目录中导入邮件

打开“从OE6导入”对话框，单击选中“从OE6存储目录中导入邮件”单选按钮。



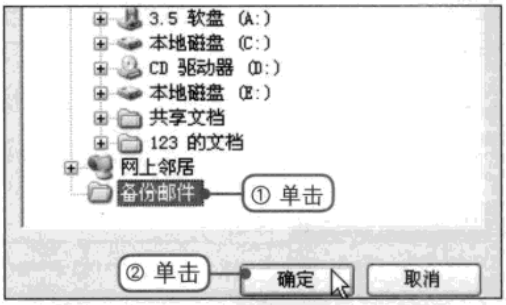
④ 单击“浏览”按钮

单击“确定”按钮返回“Outlook Express导入”对话框，单击“浏览”按钮。



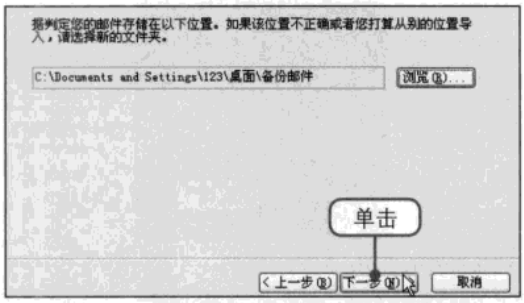
⑤ 选择导入邮件的所在位置

弹出“浏览文件夹”对话框，①在下方的列表框中单击选中“备份邮件”文件夹。②单击“确定”按钮。



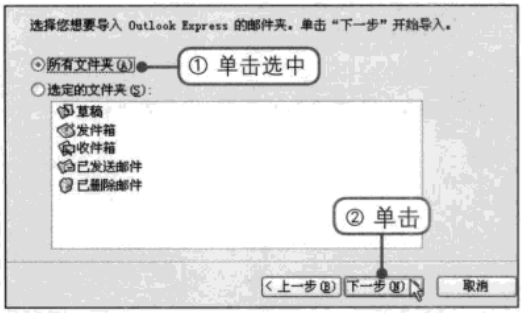
⑥ 确定选择的导入邮件位置

返回“Outlook Express导入”对话框，在对话框中确认选择的导入邮件位置无误后单击“下一步”按钮。



⑦ 选择文件夹

打开“选择文件夹”对话框，①单击选中“所有文件夹”单选按钮。②单击“下一步”按钮。



⑧ 导入完成

接着打开“导入完成”对话框，直接单击“完成”按钮即可。

6.7 备份与还原“IE 收藏夹”

目前常用的IE6和IE7浏览器都提供了导入/导出功能，即备份/还原功能，它可以很快速地将收藏夹中的所有网页记录导出到计算机上的其他应用程序或者文件中，然后将其存储在一个安全目录中。收藏夹导出后是一个HTML格式的网页文件，双击打开该网页文件，然后单击其中的网页链接可打开对应的网页。当用户在重新安装操作系统或者重新安装IE浏览器之前都需要首先对浏览器中的收藏夹进行导出操作以防止丢失某些网页。安装后安装将其导入浏览器即可。

6.7.1 备份“IE收藏夹”

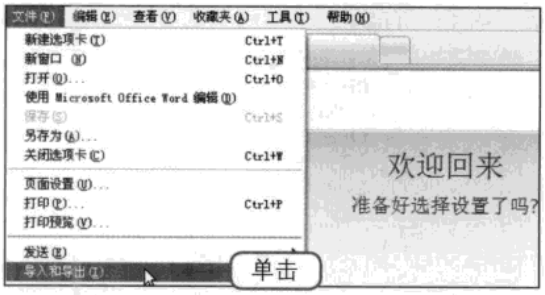
备份IE收藏夹是指通过IE浏览器的导入/导出功能将IE收藏夹以HTML格式的文件备份至电脑的磁盘中。

① 启动IE浏览器

双击桌面上的Internet Explorer快捷图标，启动IE浏览器，打开浏览器窗口。

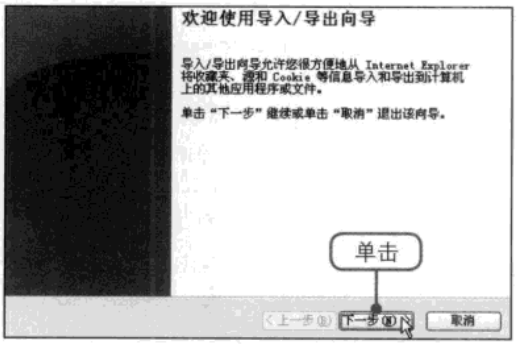
② 单击“导入和导出”命令

单击菜单栏中的“文件>导入和导出”命令。



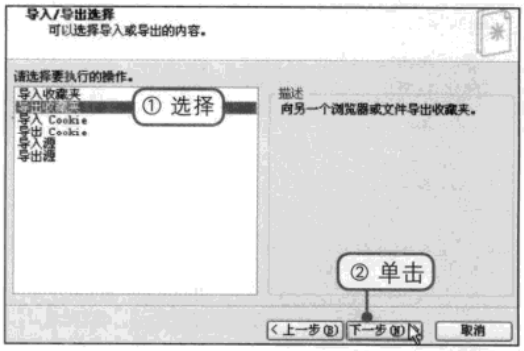
③ 单击“下一步”按钮

打开“欢迎使用导入/导出向导”对话框，直接单击“下一步”按钮。



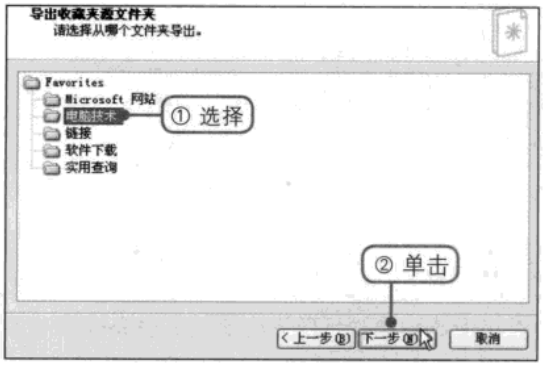
④ 选择导出收藏夹

弹出“导入/导出选择”对话框，①在“请选择要执行的操作”列表框中选择“导出收藏夹”选项。②单击“下一步”按钮。



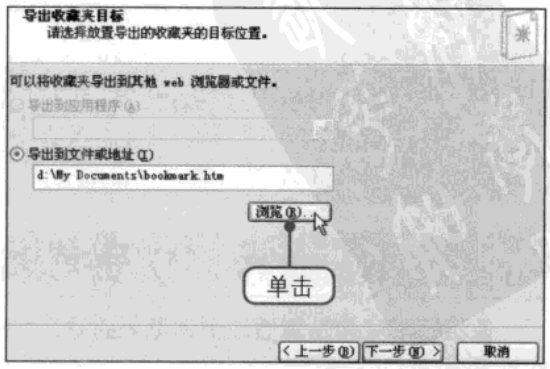
⑤ 选择导出收藏夹的文件夹

①在打开的对话框中选择导出的文件夹。②单击“下一步”按钮。



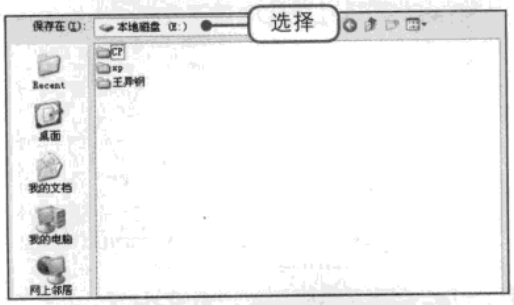
⑥ 单击“浏览”按钮

弹出“导出收藏夹目标”对话框，单击“浏览”按钮。



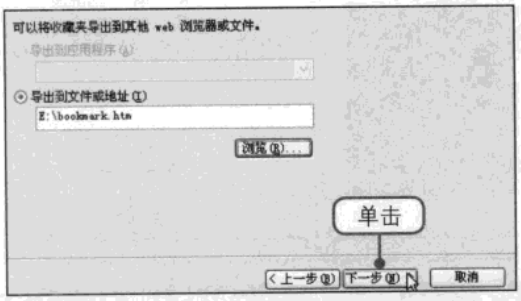
⑦ 选择书签文件

打开“请选择书签文件”对话框，在“保存在”下拉列表中选择备份文件的保存位置，接着在下方的“文件名”文本框中输入名称，单击“确定”按钮。



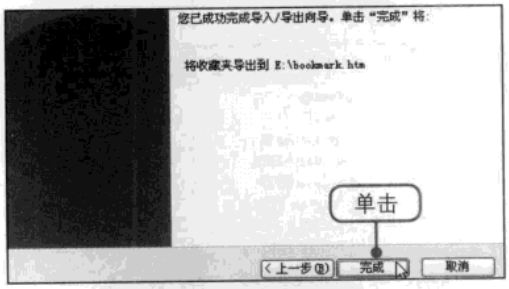
⑧ 确认选择的保存位置

返回“导出收藏夹目标”对话框，确认选择的保存位置无误后单击“下一步”按钮。



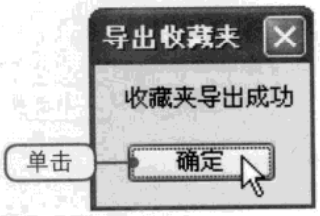
⑨ 完成导出

打开“正在完成导入/导出向导”对话框，单击“完成”按钮。



⑩ 导出成功

弹出“导出收藏夹”提示框，提示用户收藏夹导出成功，直接单击“确定”按钮退出即可。

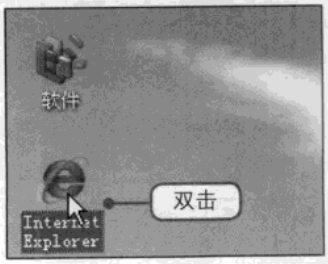


6.7.2 还原“IE收藏夹”

用户重新安装了系统或者IE浏览器之后，便可使用导入/导出功能还原IE收藏夹。

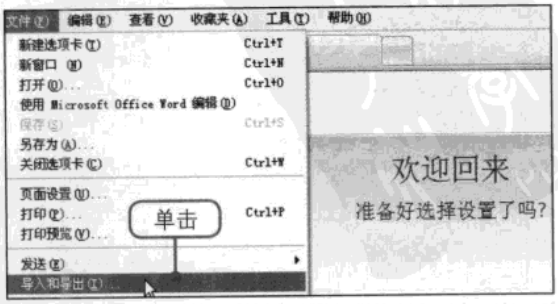
① 启动IE浏览器

双击桌面上的Internet Explorer快捷图标，启动IE浏览器，打开浏览器窗口。



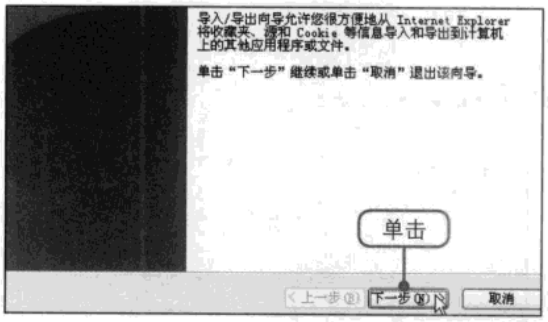
② 单击“导入和导出”命令

单击菜单栏中的“文件>导入和导出”命令。



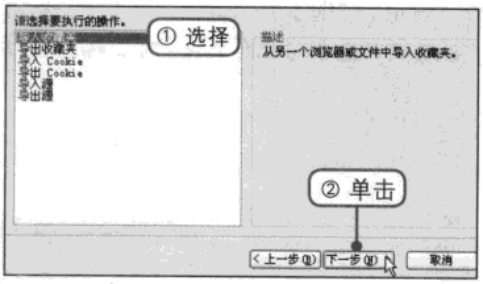
③ 单击“下一步”按钮

打开“欢迎使用导入/导出向导”对话框，直接单击“下一步”按钮。



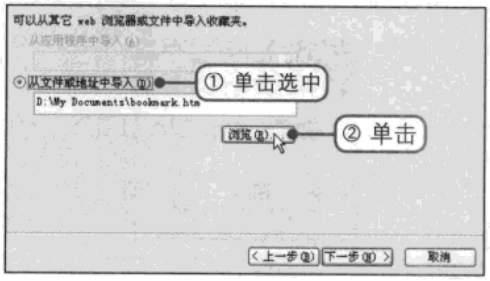
④ 选择导入收藏夹

打开“导入/导出选择”对话框，①在“请选择要执行的操作”列表框中选择“导入收藏夹”选项。②单击“下一步”按钮。



⑤ 单击“浏览”按钮

打开“导入收藏夹的来源”对话框，①单击选中“从文件或地址中导入”单选按钮。②单击下方的“浏览”按钮。

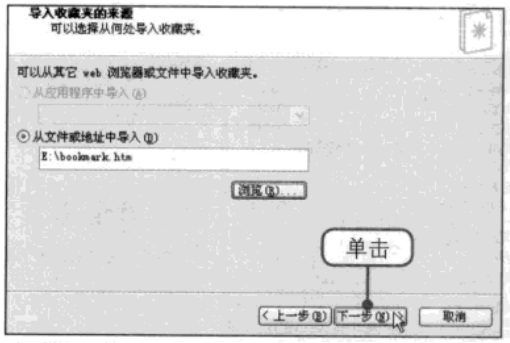


⑥ 选中备份的IE收藏夹文件

打开“请选择书签文件”对话框，①在“查找范围”下拉列表中选择备份文件保存的位置。②在下方列表框中单击以选中文件并单击“打开”按钮。

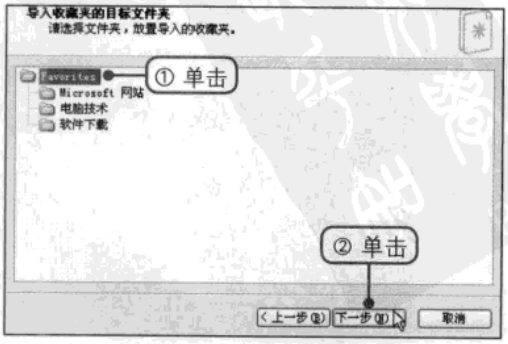
⑦ 确认选择的保存位置

返回“导入收藏夹的来源”对话框，确认选择的保存位置正确无误后单击“下一步”按钮。



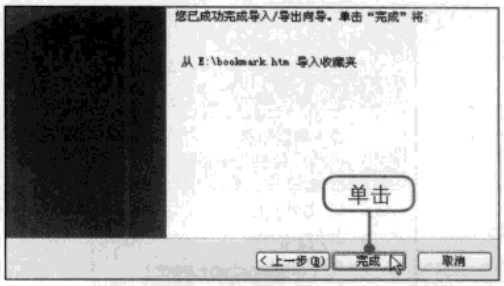
⑧ 选择放置导入的文件夹

打开“导入收藏夹的目标文件夹”对话框，①在列表框中单击以选中放置导入的文件夹。②单击“下一步”按钮。



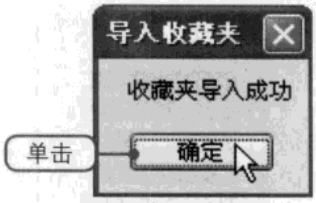
⑨ 完成导入

打开“正在完成导入/导出向导”对话框，单击“完成”按钮。



⑩ 导入成功

弹出“导入收藏夹”提示框，提示用户收藏夹导入成功，直接单击“确定”按钮退出即可。



6.8 备份与还原QQ聊天记录

当使用QQ聊天时，QQ聊天记录默认存放在消息管理器中。对某些用户来说，有些QQ聊天记录是非常重要的，当重新安装了操作系统或者QQ软件后就会导致这些重要的数据丢失，为此，应先对重要的QQ聊天记录进行备份操作，然后再重新安装操作系统或者QQ之后将备份文件导入即可避免丢失。

6.8.1 备份QQ聊天记录

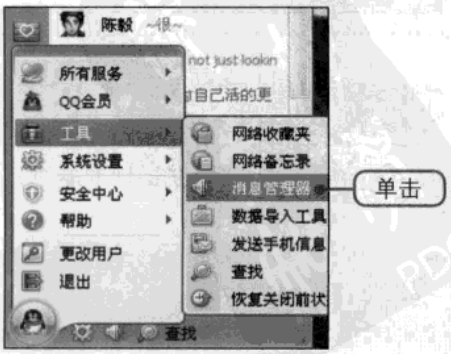
下载并安装好QQ应用软件之后，使用QQ聊天的过程中该软件会自动将其聊天信息记录在消息管理器中，若用户需要查找一段时间之前的聊天记录，可通过消息管理器进行查找。但是为了安全起见，需要将重要的聊天记录备份。

① 单击“系统菜单”按钮

打开QQ应用程序登录界面并成功登录之后，单击QQ主界面下方的“主菜单”按钮。

② 单击“消息管理器”命令

在弹出的菜单中单击“工具>消息管理器”命令。



③ 选择需要备份聊天记录的好友

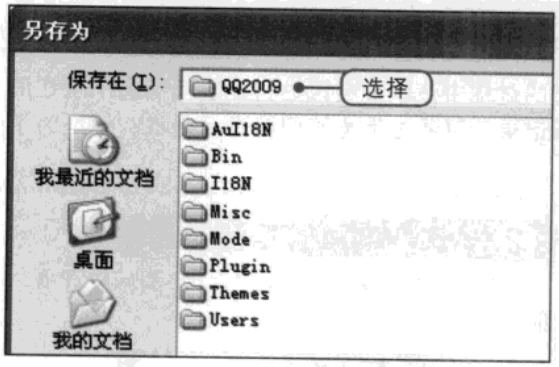
打开“信息管理器”窗口，在左侧任务窗格中选择需要备份的QQ好友。

④ 单击“导出消息记录”命令

①在窗口左上角单击“导入和导出”按钮。
②在弹出的菜单中单击“导出消息记录”命令。

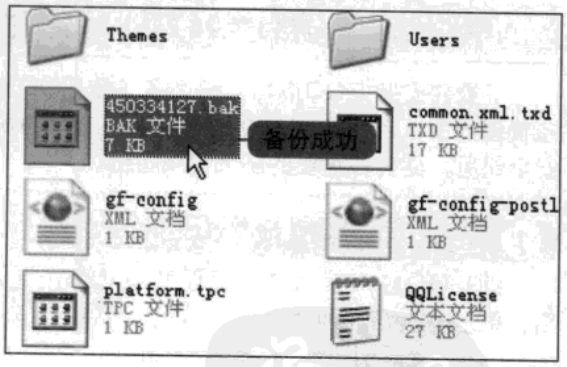
⑤ 选择备份文件的保存位置

弹出“另存为”对话框，在“保存在”下拉列表中选择备份文件的保存位置。



⑥ 备份成功

单击“保存”按钮返回窗口，打开备份文件所在的窗口即可看见导出的文件。

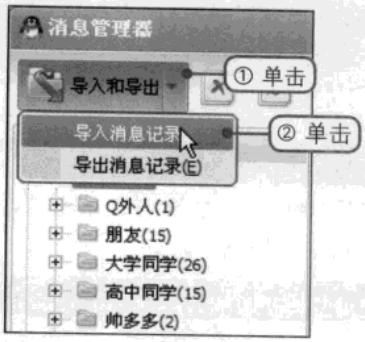


6.8.2 还原QQ聊天记录

当QQ软件或者系统出现问题时，用户可在重新安装了对应的软件之后导入聊天记录即可。

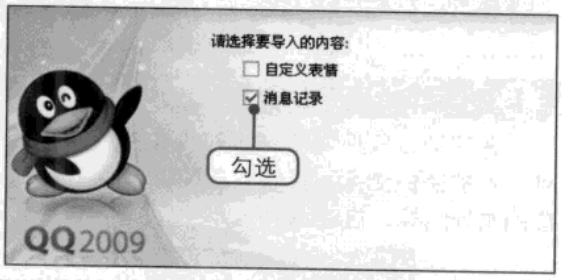
① 单击“导入消息记录”命令

打开消息管理器窗口，①单击“导入和导出”按钮。②在弹出的菜单中单击“导入消息记录”命令。



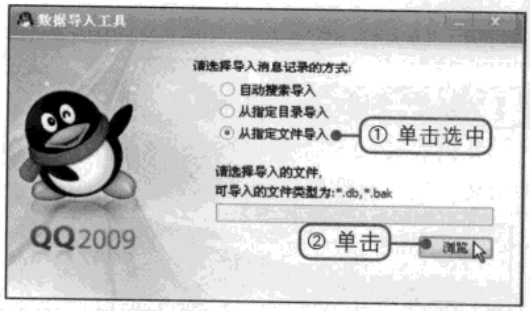
② 导入消息记录

弹出“数据导入工具”对话框，勾选“消息记录”复选框，然后单击“下一步”按钮。



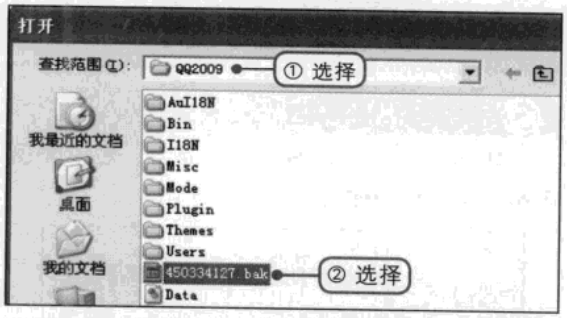
③ 从指定文件导入

①在打开的新界面中单击选中“从指定文件导入”单选按钮。②单击“浏览”按钮。



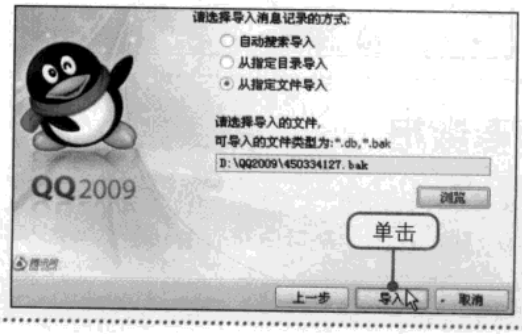
④ 导出成功

弹出“打开”对话框，①在“查找范围”下拉列表中选择备份文件所在的位置。②在下方的列表框中选择备份的文件。



⑤ 开始导入

返回“数据导入工具”对话框，确认选择的文件无误后单击“导入”按钮。



⑥ 导入成功

片刻之后导入成功，直接单击“完成”按钮退出即可。

6.9 重要数据刻录保护

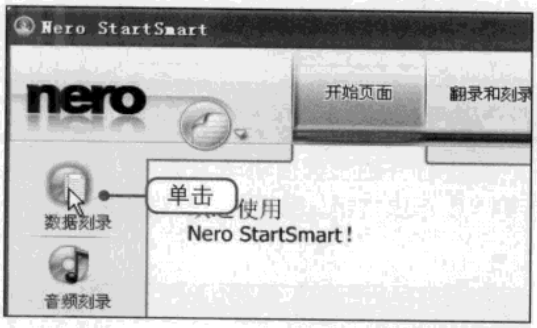
可以将存储在电脑中的重要数据刻录成光盘，这样一来即使电脑出现故障数据也不会丢失。使用功能比较强大的Nero刻录软件，不但能够将重要数据刻录到空白光盘中，还可以将重要数据刻录成镜像文件，直接通过虚拟光驱即可打开。

① 启动Nero应用软件

在启动该软件之前，应在光驱中放入一张可写入的空白光盘，接着双击Nero刻录软件对应的快捷图标，启动Nero应用软件。

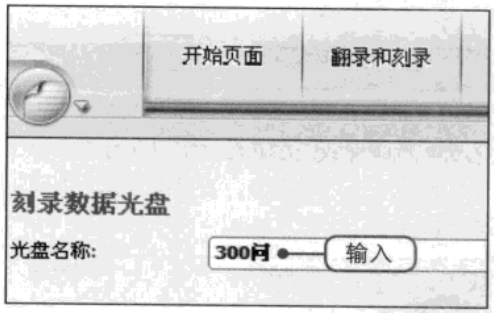
② 选择数据刻录

打开Nero主界面窗口，单击“数据刻录”图标，启动数据刻录。



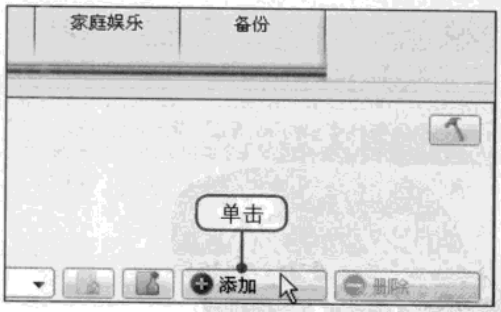
③ 设置光盘名称

切换至“刻录数据光盘”界面，在“光盘名称”文本框中输入光盘的名称。



④ 单击“添加”按钮

单击右侧的“添加”按钮。打开“添加文件和文件夹”对话框。

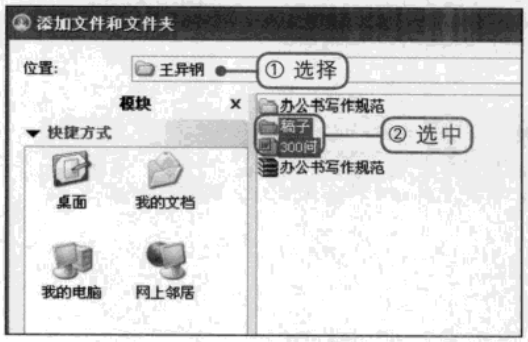


使用DVD光驱直接刻录重要数据

用户可直接使用DVD光驱刻录重要数据，即首先将一张可写入的空白光盘放入光驱，接着将重要数据对应的图标拖动至“我的电脑”窗口中对应的光驱图标即可实现刻录，但前提是电脑上的光驱具有刻录功能。

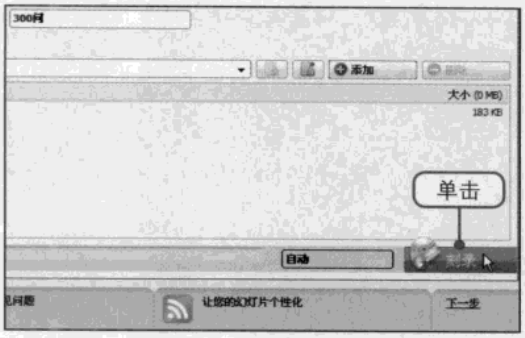
5 选择重要数据

①在“位置”下拉列表中选择重要数据所在的文件夹。②在下方的列表框中选中需要刻录保护的重要数据。若要选择多个文件，则可先选中一个，接着按住Ctrl键不放继续选择其他的文件或文件夹。



6 开始刻录

返回主界面窗口，确认选择的文件正确无误后单击右下方的“刻录“按钮开始刻录，请耐心等待，刻录完成后取出光盘即可。



读书笔记

Chapter 07

实现安全上网

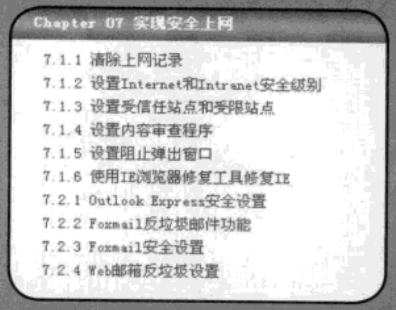
重点知识

1. 设置IE浏览器
2. 通信安全

随着因特网的推广及应用，实现安全上网对维护电脑安全是十分重要的。Internet Explorer浏览器是Windows操作系统自带的，是使用最广泛的网页浏览器，若要实现安全上网就需要安全的设置IE浏览器，当IE浏览器出现问题时就需要用户手动及时修复。除此之外，用户所使用的邮箱也要进行安全设置，如Foxmail和Outlook Express等软件，用户可参照本章的内容对它们进行安全设置。

视频文件

参见随书光盘：视频教程\Chapter 07



7.1 设置IE浏览器

IE浏览器，全称为Internet Explorer浏览器，是微软公司推出的一款网页浏览器，当安装了Windows操作系统后，桌面上就会出现对应的Internet Explorer图标，它是使用最广泛的网页浏览器。用户在使用IE浏览器之前需要对其进行相关的设置，保障浏览器的安全。

7.1.1 清除上网记录

当使用IE浏览器打开并浏览网页时，IE浏览器自动记忆了用户浏览的网页和相关信息，为了防止其他用户偷窥重要的信息，如通过Cookie偷窥账号和密码等信息，在关闭浏览器之前应该清除上网记录。

① 启动IE浏览器

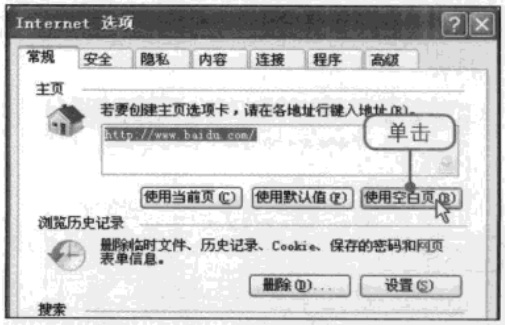
在桌面上双击Internet Explorer快捷图标，启动IE浏览器。

② 单击“Internet选项”命令

打开IE浏览器窗口，在菜单栏中单击“工具>Internet选项”命令。

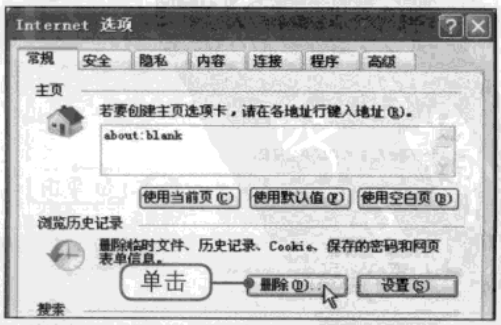
③ 设置主页

打开“Internet选项”对话框，在“主页”选项组中单击“使用空白页”按钮。



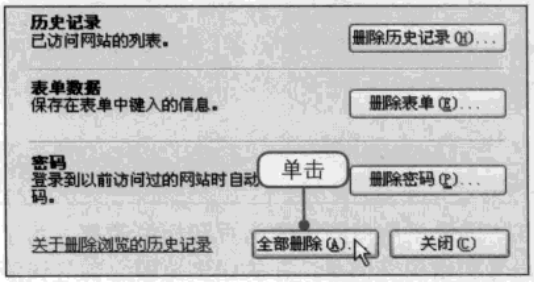
④ 单击“删除”按钮

在“浏览历史记录”选项组中单击“删除”按钮。



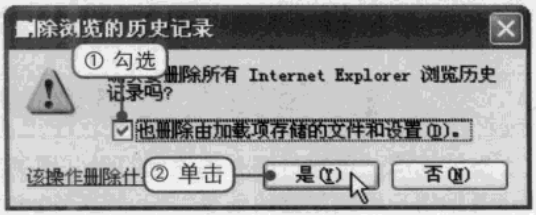
⑤ 删除浏览的历史记录

弹出“删除浏览的历史记录”对话框，用户可根据自身的情况选择需要删除的历史记录，例如单击“全部删除”按钮。



⑥ 确认删除

弹出“删除浏览的历史记录”对话框，①勾选“也删除由加载项存储的文件和设置”复选框。②单击“是”按钮即可清除。

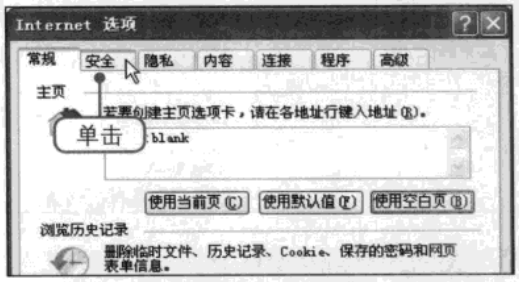


7.1.2 设置Internet和Intranet安全级别

用户可继续在“Internet选项”对话框中的“安全”选项卡下设置IE浏览器的Internet和Intranet安全级别。

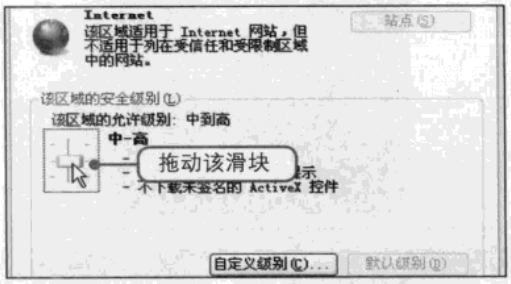
① 切换至“安全”选项卡

按照前面的方法打开“Internet选项”对话框，单击“安全”标签切换至该选项卡。



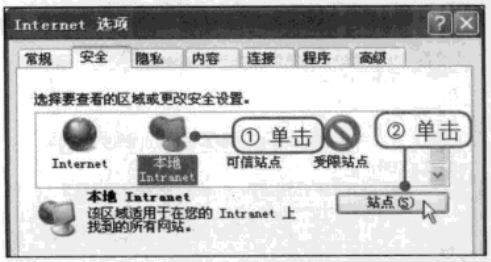
② 设置Internet的安全级别

在“该区域的安全级别”选项组中拖动滑块至“中—高”选项处。



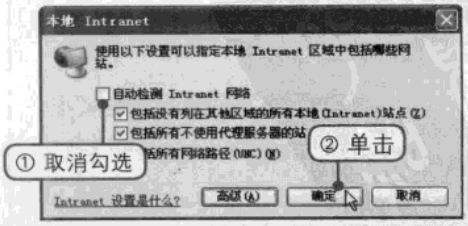
③ 单击“站点”按钮

①单击选中“本地Intranet”选项。②单击“站点”按钮。



④ 设置本地Intranet

弹出“本地Intranet”对话框，①取消勾选“自动检测Intranet网络”复选框。②单击“确定”按钮。



⑤ 设置本地Intranet的安全级别

返回“Internet选项”对话框，在“该区域的安全级别”选项组中拖动滑块至“中”选项处。

新手学堂 本地Intranet

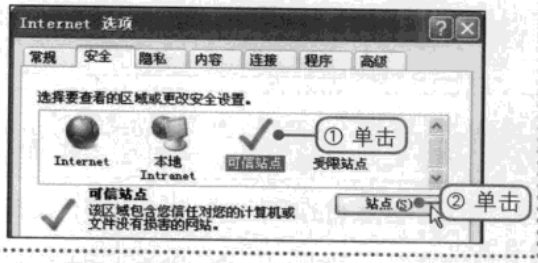
Intranet，被称作企业内部网，是一种通常用于公司或组织内部的专用网络，与Internet相比，Internet是面向全球的网络，而Intranet则是Internet技术在企业机构内部的实现。Intranet用于存储内部与公司的相关信息，例如有关公司策略或者员工福利的信息，因为由管理员严格控制安全，所以Intranet的安全设置可能比Internet的安全设置稍微差了一点。

7.1.3 设置受信任站点和受限站点

如果认为某一网站会破坏电脑的重要数据或者系统，可通过设置受限站点将其加入受限站点中来拒绝访问，相反可通过设置受信任站点将其加入可信站点。

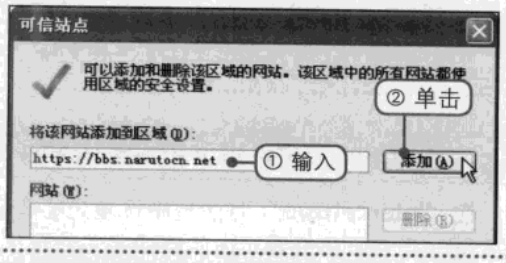
① 单击“站点”按钮

按照前面的方法打开“Internet选项”对话框。①在“安全”选项卡中单击“可信站点”选项。②单击“站点”按钮。



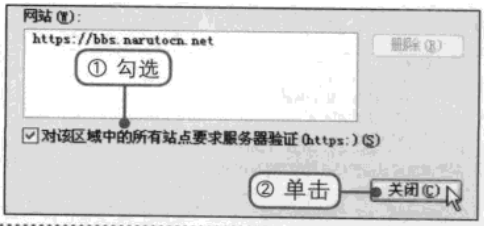
② 添加可信站点

弹出“可信站点”对话框，①在“将该网站添加到区域”文本框中输入可信站点的网站。②单击右侧的“添加”按钮。



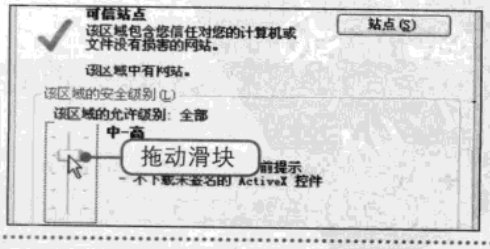
③ 设置服务器验证

①勾选“对该区域中的所有站点要求服务器验证”复选框。②单击“关闭”按钮。



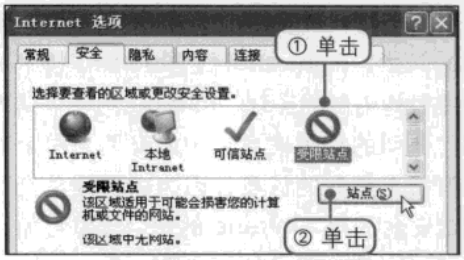
④ 设置可信站点的安全级别

返回“Internet选项”对话框，拖动滑块至“中—高”选项处。



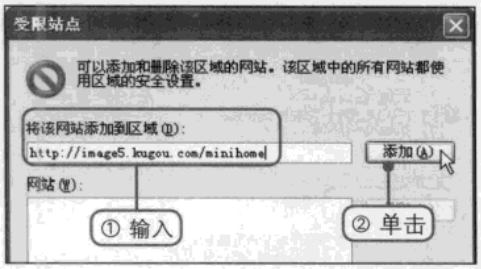
⑤ 单击“站点”按钮

①在“Internet选项”对话框中单击“受限站点”选项。②单击下方的“站点”按钮。



⑥ 设置受限站点

弹出“受限站点”对话框，①在“将该网站添加到该区域”文本框中输入受限站点的网站。②单击“添加”按钮。

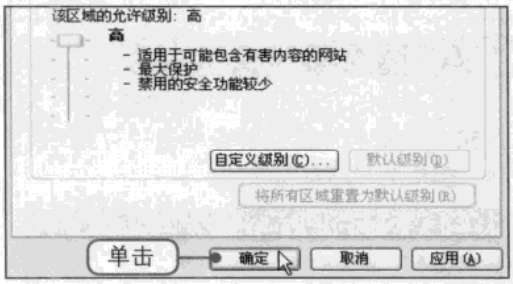


⑦ 单击“关闭”按钮

接着可在“网站”列表框中看见添加的受限网站，直接单击“关闭”按钮关闭该对话框。

⑧ 保存退出

返回“Internet选项”对话框，可单击“默认级别”按钮查看受限站点的安全级别，默认设置为高，接着单击“确定”按钮即可。

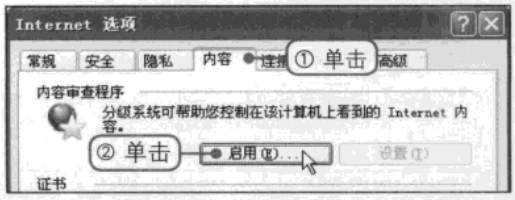


7.1.4 设置内容审查程序

在“Internet选项”对话框中设置内容审查程序，即对一些敏感的词语进行分级设置，设置之后系统会要求用户设置对应的密码来防止他人更改设置。

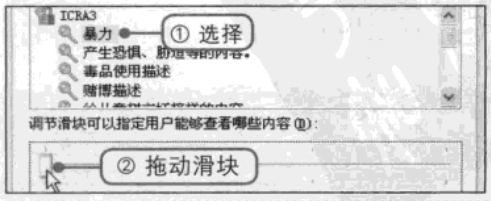
① 启用内容审查程序

打开“Internet选项”对话框，①单击“内容”标签切换至该选项卡。②在“内容审查程序”选项组中单击“启用”按钮。



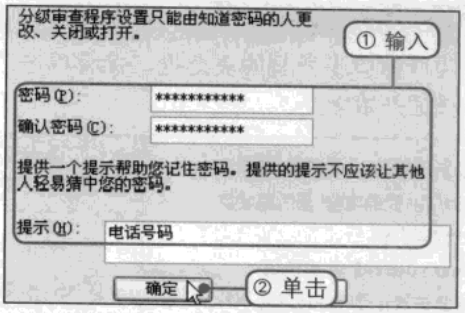
② 设置分级级别

弹出“内容审查程序”对话框，①在列表框中选择“暴力”选项。②在下方将滑块拖动至最左边，然后单击“确定”按钮。



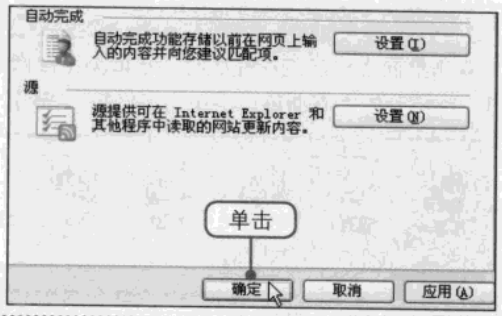
③ 设置密码

弹出“创建监护人密码”对话框，①在对话框中输入设置的密码和密码提示。②单击“确定”按钮。



④ 保存退出

弹出“内容审查程序”对话框，直接单击“确定”按钮返回“Internet选项”对话框，单击下方的“确定”按钮保存退出。

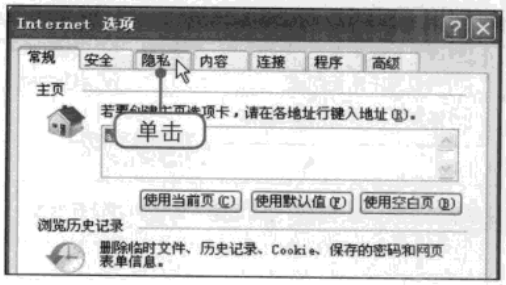


7.1.5 设置阻止弹出窗口

当用户在浏览网页时，有时会弹出一些小Web窗口，这些窗口就是弹出窗口。阻止弹出窗口是IE浏览器中的功能，可使用户限制或阻止大多数弹出窗口。

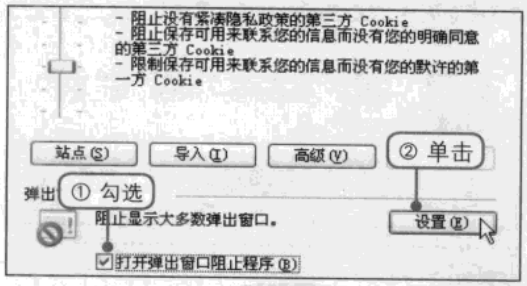
① 切换至“隐私”选项卡

按照前面的方法打开“Internet选项”对话框，单击“隐私”标签切换至该选项卡。



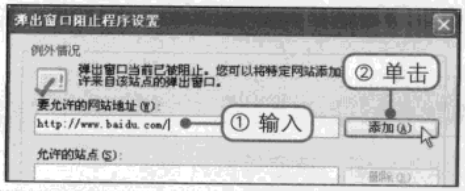
② 单击“设置”按钮

①勾选“打开弹出窗口阻止程序”复选框。②单击“设置”按钮。



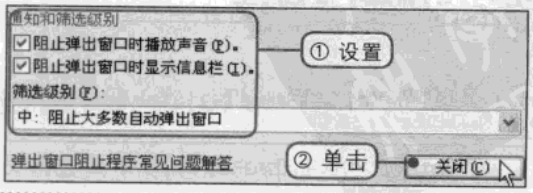
③ 添加允许的网站地址

弹出“弹出窗口阻止程序设置”对话框，①在“要允许的网站地址”文本框中输入网站地址。②单击“添加”按钮。



④ 通知和筛选级别

①在“通知和筛选级别”选项组中勾选所有的复选框并设置筛选级别为中。②单击“关闭”退出即可。

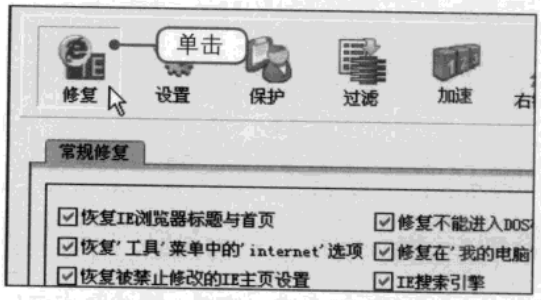


7.1.6 使用IE浏览器修复工具修复IE

当IE浏览器受到破坏而无法使用时，用户可使用IE浏览器修复工具将IE浏览器修复至最初的状态。本节以IE浏览器修复工具V3.0版本为例介绍修复方法。

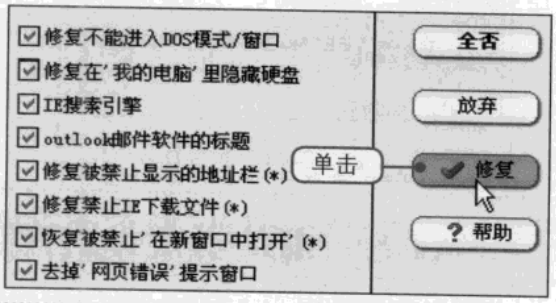
① 单击“修复”按钮

双击桌面上对应的快捷图标启动IE浏览器修复工具，在打开的主界面窗口中单击“修复”按钮。



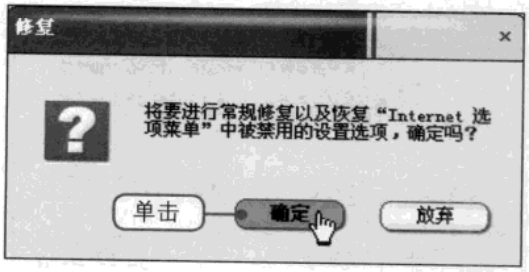
② 开始修复

勾选窗口中所有的复选框，接着单击“修复”按钮开始修复。



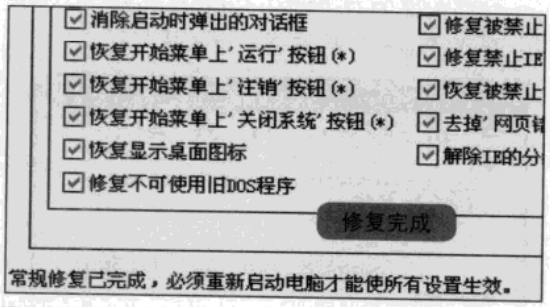
③ 确认修复

弹出“修复”提示框，直接单击“确定”按钮确认修复。



④ 修复完成

此时可在窗口的最下方看见“常规修复已完成”等字样，重新启动电脑即可。



7.2 通信安全

连接互联网除了浏览网页之外，还可以与他人进行通信，但是在通信的过程中，同样也会遭受病毒、黑客的入侵，因此需要对通信软件进行相关的设置，通信软件除了聊天软件之外，电子邮箱也是重要的通信工具，用户在使用它们时也要对其进行安全设置。

7.2.1 Outlook Express安全设置

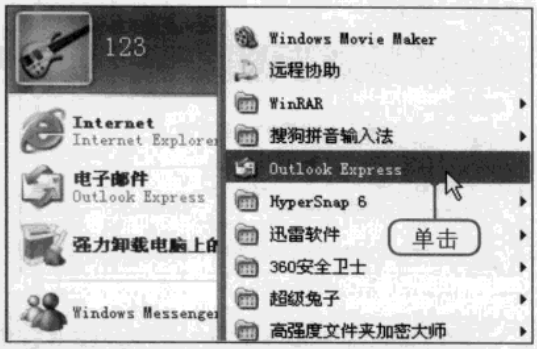
在使用Outlook Express时需要对其进行安全设置，以防病毒、黑客等的入侵。

① 单击“所有程序”命令

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“所有程序”命令。

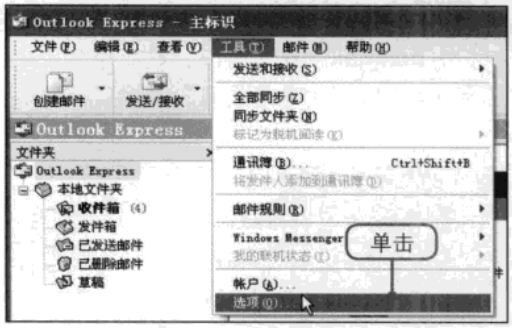
② 启动Outlook Express

在弹出的菜单中单击Outlook Express命令，启动Outlook Express应用程序。



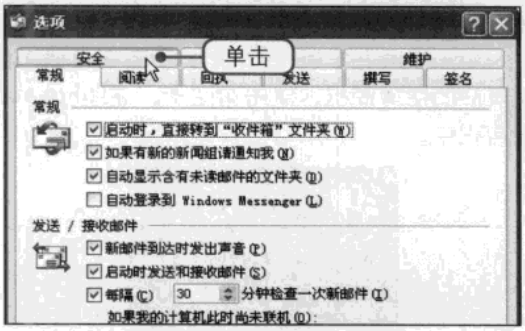
③ 单击“选项”命令

打开Outlook Express主界面窗口，在菜单栏中单击“工具>选项”命令。



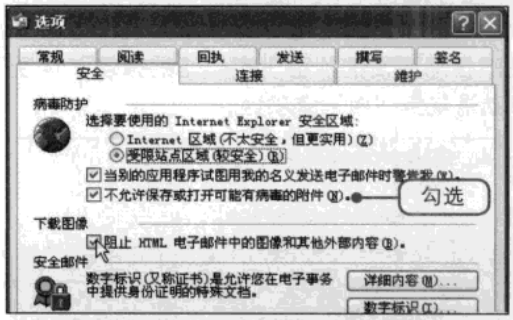
④ 切换至“安全”选项卡

打开“选项”对话框，单击“安全”标签切换至该选项卡。



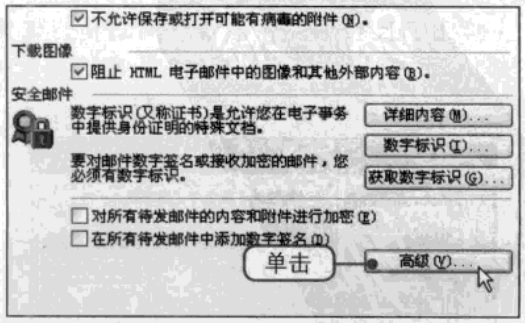
⑤ 设置病毒防护

在“病毒防护”选项组中勾选“不允许保存或打开可能有病毒的附件”复选框。



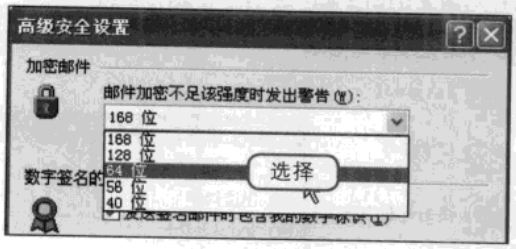
⑥ 单击“高级”按钮

在“安全邮件”选项组中单击“高级”按钮。



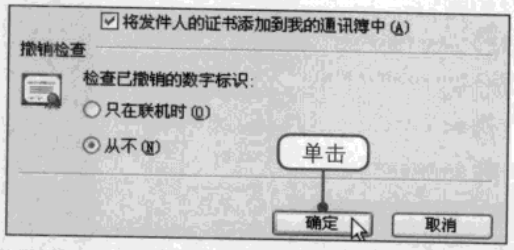
⑦ 设置加密邮件

弹出“高级安全设置”对话框，在“邮件加密不足该强度时发出警告”下拉列表中选择“64位”选项。



⑧ 保存退出

单击“确定”按钮返回“选项”对话框，再次单击“确定”按钮保存退出。

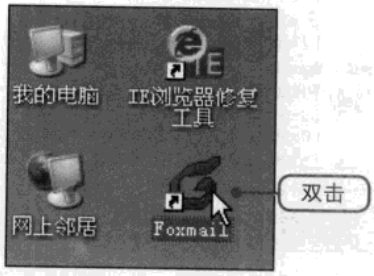


7.2.2 Foxmail反垃圾邮件功能设置

Foxmail是一款优秀的国产电子邮件客户端软件，它具备强大的反垃圾邮件功能，并且能够使用多种技术进行判别垃圾邮件和非垃圾邮件。

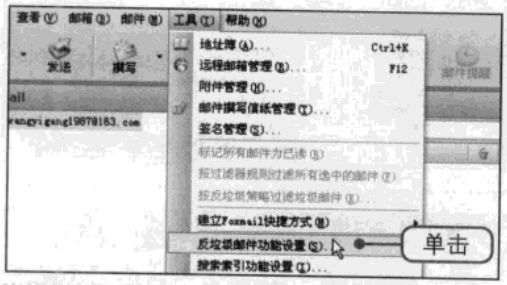
① 启动Foxmail应用程序

用户下载并安装好Foxmail后会在桌面上出现对应的快捷图标，双击该图标，启动Foxmail应用程序。



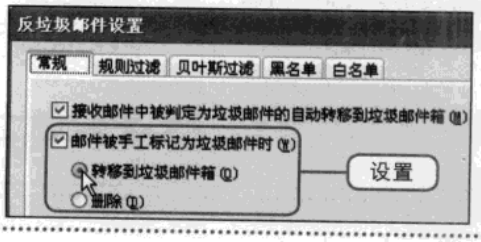
② 单击“反垃圾邮件功能设置”命令

打开Foxmail主界面窗口，在菜单栏中单击“工具>反垃圾邮件功能设置”命令。



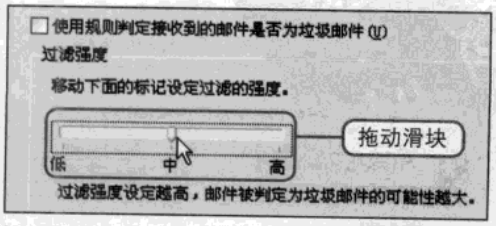
③ 常规设置

弹出“反垃圾邮件设置”对话框，勾选“邮件被手工标记为垃圾邮件时”复选框并单击选中“转移到垃圾邮件箱”单选按钮。



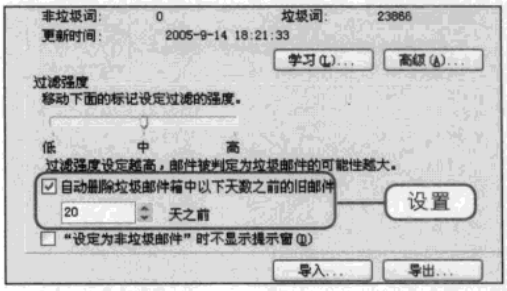
④ 规则规律设置

单击“规则过滤”标签切换至该选项卡，在“移动下面的标记设定过滤的强度”选项下拖动滑块至“中”选项处。



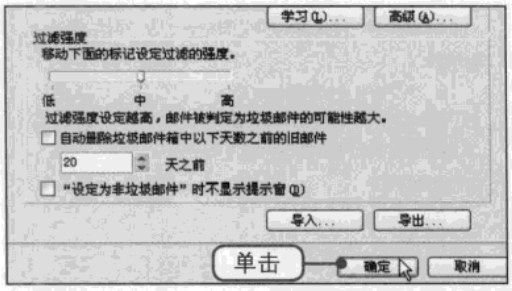
⑤ 设置邮件的保存时间

切换至“贝叶斯过滤”选项卡下，勾选“自动删除垃圾邮件箱中以下天数之前的旧邮件”复选框并在下方设置对应的时间。



⑥ 保存退出

设置完成后直接单击“确定”按钮保存退出即可。

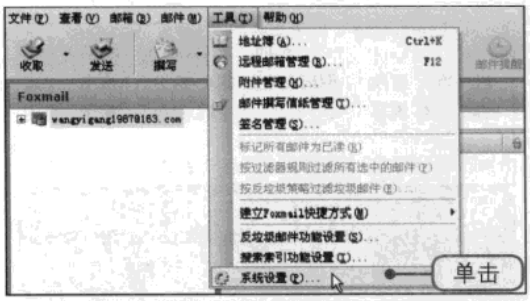


7.2.3 Foxmail安全设置

用户除了对Foxmail进行反垃圾邮件设置外，还需要对其进行安全设置以保障其安全。

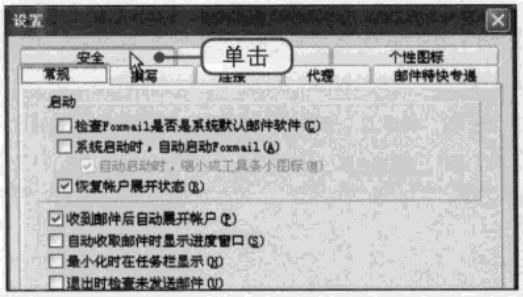
① 单击“系统设置”命令

打开Foxmail主界面窗口，在菜单栏中单击“工具>系统设置”命令。



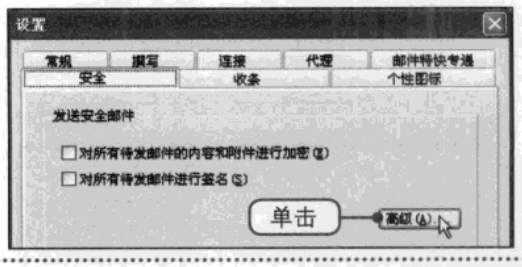
② 切换至“安全”选项卡

打开“设置”对话框，单击“安全”标签切换至该选项卡。



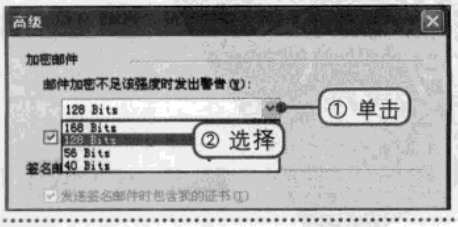
③ 单击“高级”按钮

在“发送安全邮件”选项组中单击下方的“高级”按钮，弹出“高级”对话框。



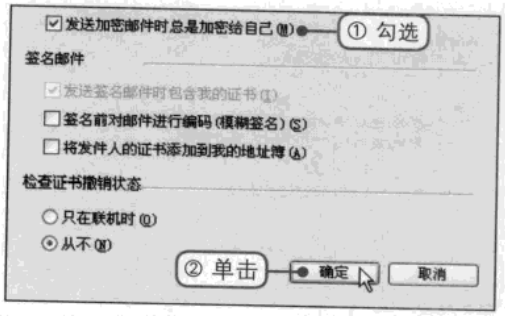
④ 设置邮件加密强度

①单击“邮件加密不足该强度时发出警告”右侧的下三角按钮。②在弹出的下拉列表中选择“128bits”选项。



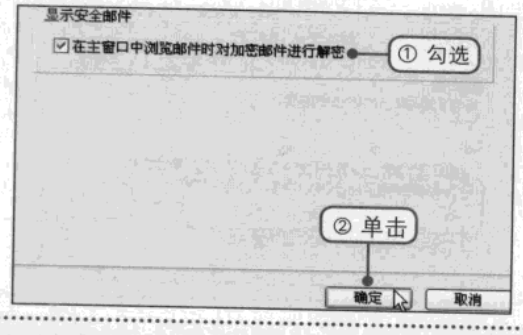
⑤ 设置发送加密邮件时总是加密给自己

①勾选“发送加密邮件时总是加密给自己”复选框。②单击“确定”按钮。



⑥ 配置系统

返回“设置”对话框，①勾选“在主窗口中浏览邮件时对加密文件进行解密”复选框。②单击“确定”按钮保存退出。

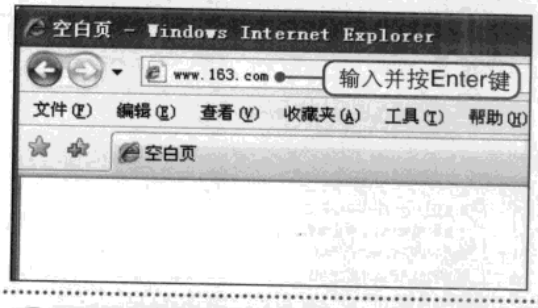


7.2.4 Web邮箱反垃圾设置

当用户在使用Web邮箱时也需要注意识别垃圾邮件。可登录Web邮箱进行反垃圾邮件的设置。

① 打开网易首页

打开IE浏览器窗口，在窗口中输入www.163.com并按Enter键。



② 单击“免费邮箱”文字链接

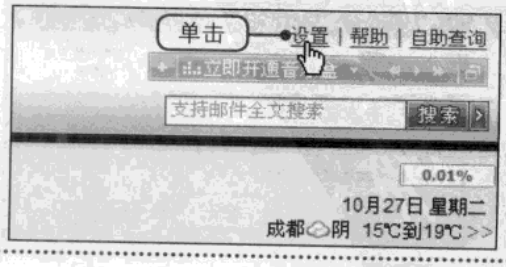
打开网易首页，在页面中单击顶部的“免费邮箱”文字链接。

③ 登录网易邮箱

①在打开的界面中选择邮箱类型并输入用户名和密码。②单击“登录”按钮。

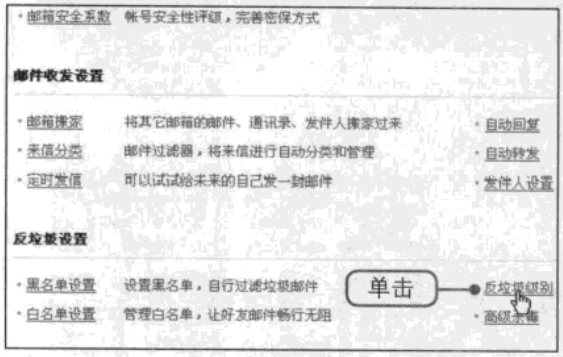
④ 单击“设置”文字链接

成功登录后打开电子邮箱首页，在页面的右上角单击“设置”文字链接。



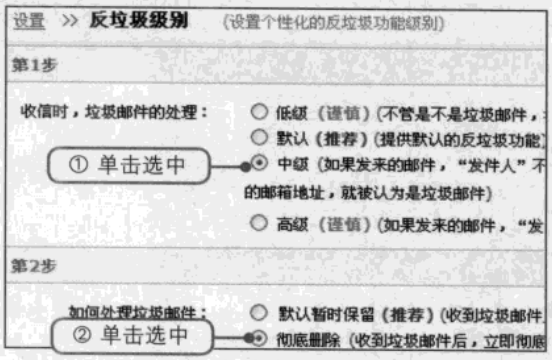
⑤ 单击“反垃圾级别”文字链接

打开“邮箱设置”页面，在“反垃圾设置”选项组中单击“反垃圾级别”文字链接。



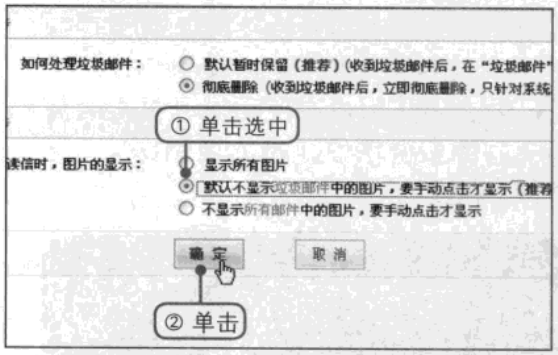
⑥ 设置反垃圾级别

①在“收信时，垃圾邮件的处理”选项组中单击选中“中级”单选按钮。②在“如何处理垃圾邮件”选项组中单击选中“彻底删除”单选按钮。



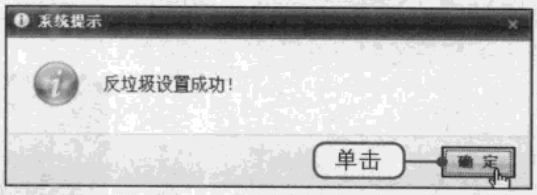
⑦ 设置读信时的图片显示

①在“读信时，图片的显示”选项组中单击选中“默认不显示”单选按钮。②单击“确定”按钮。



⑧ 保存退出

此时弹出“系统提示”对话框，提示用户反垃圾设置成功，直接单击“确定”按钮保存退出即可。



读书笔记

Chapter 08

安全使用个人网上银行

重点知识

1. 认识网上银行
2. 安全登录网上银行
3. 使用个人网上银行应注意的问题
4. 加固个人网上银行的安全

随着科技和互联网的发展，网上银行的出现为人们提供了方便，用户通过网络就可以在家里完成交易，如使用网上银行付款和转账。但是由于互联网是一个开放的网络，这也为一些非法分子提供了可趁之机，通过非法的手段盗取用户的网银账号和密码，使用钓鱼网站诱骗用户等，使得用户遭受损失。因此用户在使用网上银行时需要使用各种不同的安全手段，例如使用U盾、电子银行口令卡、网银助手等。

视频文件

参见随书光盘：视频教程\Chapter 08

Chapter 08 安全使用个人网上银行

8.4.1 下载并安装“防钓鱼安全控件”
8.4.2 更改预留信息验证
8.4.3 使用小e安全检测

8.1 认识网上银行

网上银行（Internet bank or E-bank）包含两层含义，一层含义是指通过信息网络开办业务的银行；另一层是指银行通过信息网络提供的金融服务，包括传统银行业务和因信息技术应用带来的新兴业务。在日常生活和工作中，用户提及的网上银行大多数是指第二层含义，即网上银行服务的概念。

网上银行也称为网络银行、在线银行，是指银行利用互联网技术，通过互联网向客户提供开户、销户、查询、对账、行内转账、跨行转账、信贷、网上证券、投资理财等传统服务项目，使客户足不出户就能够安全便捷地管理活期和定期存款、支票、信用卡及个人投资等。可以说网上银行是在互联网上的虚拟银行柜台，由于它不受时间、空间限制，能够在任何时间（Anytime）、任何地点（Anywhere）、以任何方式（Anyhow）为客户提供金融服务，因此它也被称为“3A银行”。

一般来说，网上银行的业务主要包括基本业务、网上投资、网上购物、个人理财、企业银行及其他金融服务。

1 基本网上银行业务

商业银行所提供的基本网上银行服务包括在线查询账户余额、交易记录，下载数据，转账和网上支付等。

2 网上投资

由于金融服务市场发达，可以投资的金融产品种类众多，国外的网上银行一般提供包括股票、期权、共同基金投资和CDs买卖等多种金融产品服务。

3 网上购物

商业银行的网上银行设立的网上购物协助服务，为客户网上购物提供了方便，它也为客户在相同的服务品种上提供了优质的金融服务或相关的信息服务，加强了商业银行在传统竞争领域的竞争优势。

4 个人理财助理

个人理财助理是国外网上银行重点发展的一个服务品种。各大银行将传统银行业务中的理财助理转移到网上进行，通过网络为客户提供理财的各种解决方案，提供咨询建议或者金融服务技术的援助，极大地扩大了商业银行的服务范围，并降低了相关的服务成本。

5 企业银行

企业银行服务是网上银行服务中最重要的部分之一。企业银行服务品种比个人客户的服务品种更多，也更为复杂，对相关技术的要求也更高，所以能够为企业提供网上银行服务是商业银行实力的象征之一，一般中小网上银行或纯网上银行只能部分提供，甚至完全不提供这方面的服务。

企业银行服务一般提供账户余额查询、交易记录查询、总账户与分账户管理、转账、在线支付各种费用、透支保护、储蓄账户与支票账户资金自动划拨、商业信用卡等服务；除此之外，还包括投资服务等。部分网上银行还为企业提供网上贷款业务。

6 其他金融服务

大商业银行的网上银行均通过自身或与其他金融服务网站联合的方式，为客户提供多种金融服务产品，如保险、抵押和按揭等，以扩大网上银行的服务范围。

网上银行将改变传统银行的营销方式、经营理念和战略。它极大的降低了银行服务的成本、降低了银行软、硬件开发和维护的费用以及客户的成本，它可以在更大的范围内实现规模经济，由于网上银行具有“3A”的特性，将会拥有更广泛的客户群体。网上银行的出现也将会使传统的银行竞争格局发生变化。

8.2→ 安全登录网上银行

使用网上银行的一般流程都是首先打开银行对应的网站，然后输入账号和密码等，在该流程中，用户需要注意网站、账号和密码的安全，防范账号和密码被盗，保证安全地登录网上银行。

在登录银行对应的网站时，建议用户手动输入网站地址，切勿采用超链接方式间接访问银行网站。手动打开正确的网站地址后可将其添加至浏览器的“收藏夹”中，下次可在“收藏夹”中直接打开该网站。

在登录网上银行之前需要注意计算机的安全，可下载并安装由相关银行所提供的用于保护客户端安全的控件，并且需要及时下载并安装操作系统和浏览器安全程序的升级补丁，安装并及时更新杀毒软件，不要开启来历不明的电子邮件。

做到了以上几点，用户便可以安全地登录网上银行。

钓鱼网站

钓鱼网站通常是指不法分子未经许可，以某家银行的名义，通过互联网建立貌似银行网站或网上银行的假网页。他们借助该类网站发布虚假消息，搜集客户资料，骗取客户网上银行注册卡号（登录ID）、密码、口令等信息，进而达到非法窃取客户资金的目的。

钓鱼网站的网址与真实网站的网址较为接近，由于国内注册域名的成本非常低，一些非法用户为增强假网站的欺骗性，往往使用和真实网站网址非常相似的域名。

另外，钓鱼网站的页面形式和内容与真实网站较为相似，钓鱼网站的页面往往使用正规网站的LOGO、图表、新闻内容和链接，而且在布局和内容上与真实网站非常相似。

用户在登录网站时可采用前面介绍的方法进行登录，如手动输入网站地址，或者将真实的银行地址添加至浏览器收藏夹中，切勿通过超链接方式间接访问，建议用户不要用搜索引擎搜索银行网站的网址。也可通过其他方式找到正确的网址，例如向好友询问相关银行的网址并手动输入。

8.3 使用个人网上银行应注意的问题

在使用网上银行时不要仅仅只注意登录时的安全，在进入网上银行之后也需要注意安全，例如注册网上银行、登录和退出网上银行、设置网上密码等；另外，用户使用的电脑也需要注意安全，若电脑遭受入侵，再怎么小心都是白费精力。

以中国工商银行为例，用户安全登录了中国工商银行网站之后，接着就是注册和正常使用网上银行。

8.3.1 注册个人网上银行应注意的问题

用户在填写身份资料时不要胡乱填写，这些资料对网上银行的用户而言是十分重要的，一旦用户忘记账户密码、密码被盗或者账户受限制时，所填写的身份资料就显得十分重要了。一般情况下，能够联系到用户的通讯地址、电话、姓名等资料都必须如实填写，因为这些资料是在处理紧急情况时找到和直接证明用户身份的直接证明。否则将会造成不可估量的损失，即使一个用户拥有一种网上银行的多个账号，也要分别提供这些资料。

用户设置网上银行密码可参照第2章介绍的密码设置技巧来操作，用户在为个人的网上银行设置专门的密码时，需要注意与其他场合中（如其他网上服务、使用存折或者卡号取钱）的密码区别开来，避免因其中某一项密码丢失而导致其他密码的丢失。

当用户在注册网上银行时，需要用户输入一个有效的电子邮箱，用户输入的电子邮箱一定要可靠、迅速，最好是专用的，如果有一定条件的话，可以使用收费的邮箱，几乎所有的网上银行都声称不会向用户发送一些关于密码之类的邮件，但是为了安全起见，用户还是不要轻易打开来历不明的邮件，特别是声称是某个网上银行来的邮件，如果是带有附件的邮件，更不要轻易打开，并且不要点击其中的任何链接，这些邮件中很有可能带来木马病毒或者向客户介绍钓鱼网站，使用户造成损失。

8.3.2 使用个人网上银行应注意的问题

用户注册成功之后便可登录个人网上银行，不管是登录还是注册都需要保护账号和密码的安全，在任何时候、任何情况下，都不要将个人的账号和密码告诉别人，另外不要相信任何通过电子邮件、短信、电话等方式索要卡号和密码的行为。用户在输入密码时，可以进行多次复制和粘贴部分密码操作，以免被键盘记录器记录。粘贴的次序也可以打乱，再加上错误的字符删除，这样就没有任何一个简单的记录器能盗取了。另外网上银行一般可以提供一些加密的软键盘，目的是防键盘鼠标监听，除非对方攻破了指点数据包（是128位加密的，很难被攻破，除非是银行本身

的问题），否则是不会被盗的。最后用户必须把密码保存好，不要放在其他人容易看见的地方，也不要记录在计算机中。

有些用户喜欢一有时间就进入账户，如果进出账户的频率过高会很容易给黑客提供盗取的机会。用户一般不要通过代理进入账户，当用户使用代理服务器之后会在里面留下用户的痕迹，如果有人别有用心，会很轻松的找到用户信息。另外，用户在离开账户之后一定要确保完全退出之后方可离开，若还不放心，则可以在浏览器中删除Cookie、删除密码等历史记录，甚至可以全部删除以加强安全。

8.3.3 电脑环境的安全

由于用户登录网上银行是在电脑中运行的，所以电脑环境的安全也是至关重要的。用户应及时更新杀毒、防火墙和防黑的系统，定期检测和清理机器，保证去除各种间谍软件，另外还要在启动加载程序时明确哪些有用，哪些没有用，没有用的直接去除掉即可。

8.4 加固个人网上银行的安全

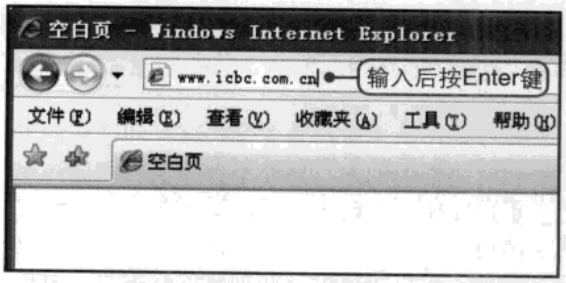
除了需要注意前面介绍的一些常用的安全措施之外，还可以使用银行提供的一些安全措施，如使用U盾、电子口令卡、小e安全检测等手段，使用户的个人网上银行安全更加的坚固。

8.4.1 下载并安装“防钓鱼安全控件”

可以通过中国工商银行网站下载并安装“防钓鱼安全控件”以防范误入钓鱼网站。

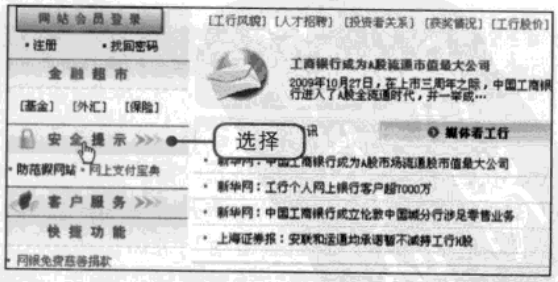
① 打开下载页面

在IE浏览器窗口的地址栏中输入www.icbc.com.cn并按Enter键。



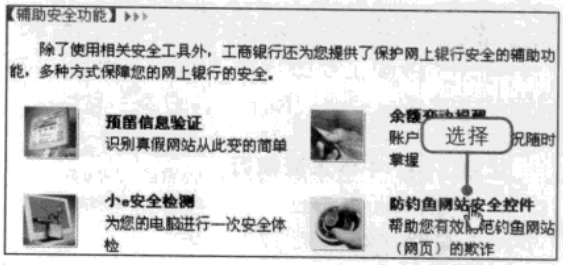
② 选择“安全提示”选项

打开“中国工商银行中国网站”页面，在页面中选择“安全提示”选项。



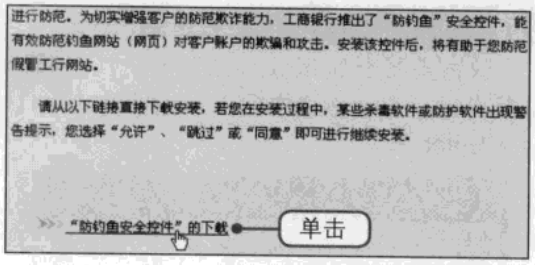
③ 选择“防钓鱼网站安全控件”选项

打开新的页面，拖动滚动条至页面底部，选择“防钓鱼网站安全控件”选项。



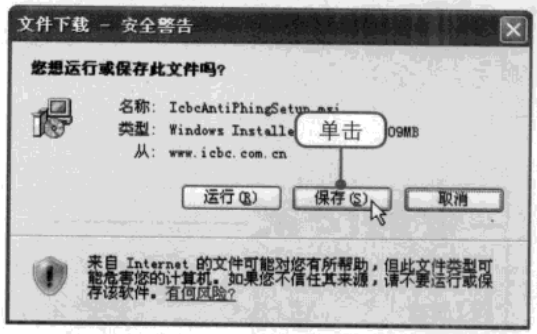
④ 开始下载

打开新的页面，在页面的底部单击“‘防钓鱼安全控件’的下载”文字链接。



⑤ 单击“保存”按钮

打开“文件下载—安全警告”对话框，单击“保存”按钮。



⑥ 选择保存路径

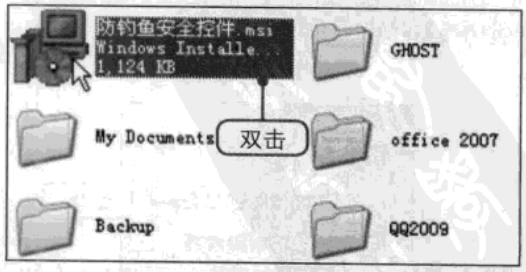
弹出“另存为”对话框，在“保存在”下拉列表中选择保存的位置。

⑦ 设置文件名

❶在对话框下方的“文件名”文本框中输入设置的文件名，例如输入“防钓鱼安全控件”。❷单击“保存”按钮。

⑧ 开始安装

下载成功之后用户可打开下载文件所在的窗口，双击对应的安装软件即可开始安装，安装只需按照向导一步步安装即可。



8.4.2 更改预留信息验证

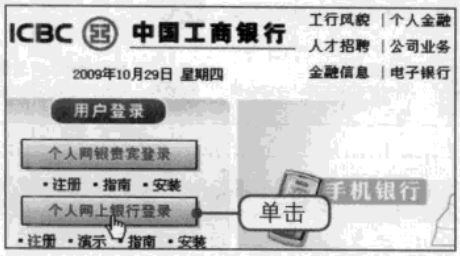
若用户想要更改预留验证信息，首先要登录个人银行，然后便可进行更改操作。

① 打开中国工商银行中国网站

双击桌面上的IE浏览器图标，打开IE浏览器窗口，在地址栏中输入www.icbc.com.cn并按Enter键。

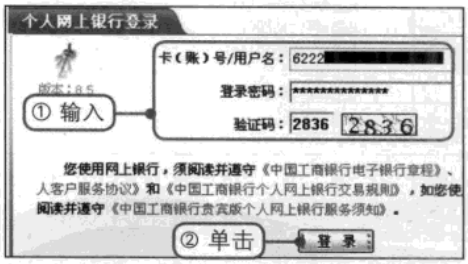
② 单击“个人网上银行登录”按钮

打开“中国工商银行中国网站”页面，在页面的左边单击“个人网上银行登录”按钮。



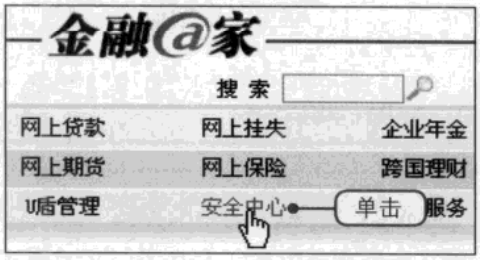
③ 输入用户名和密码

打开新的页面，①在“个人网上银行登录”选项组中的“用户名”、“登录密码”和“验证码”文本框中输入用户名、密码和验证码。②单击“登录”按钮。



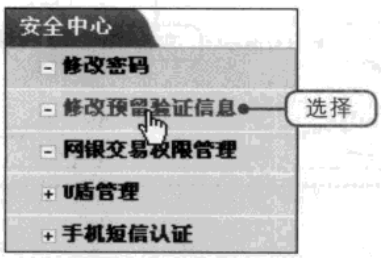
④ 单击“安全中心”文字链接

登录成功后切换至新的页面，在页面的上方单击“安全中心”文字链接。



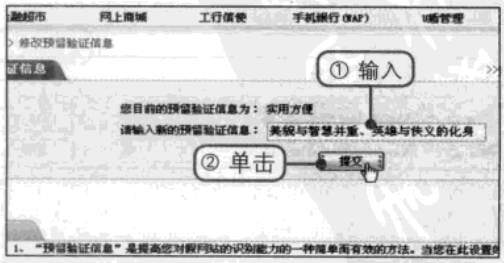
⑤ 选择“修改预留验证信息”选项

在页面的左侧选择“修改预留验证信息”选项切换至该选项卡。



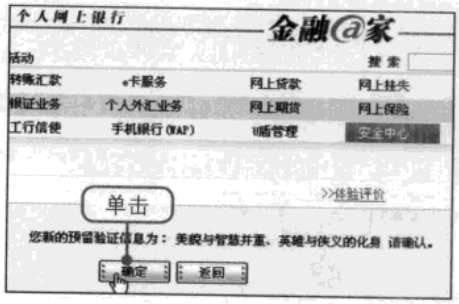
⑥ 修改预留验证信息

①在页面右侧的“请输入新的预留验证信息”文本框中输入新的预留验证信息。②单击“提交”按钮。



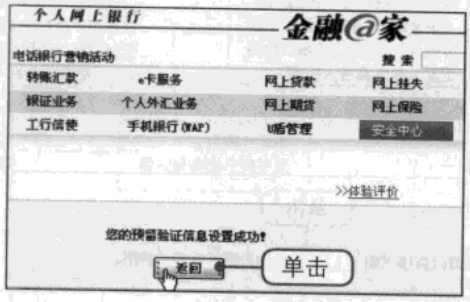
⑦ 确认设置的预留验证信息

打开新的页面，此时页面显示用户设置的预留验证信息并要求用户进行确认，确认后单击“确定”按钮。



⑧ 修改成功

切换至新的页面，此时可在页面中看见预留验证信息设置成功，单击“返回”按钮即可。



预留验证信息

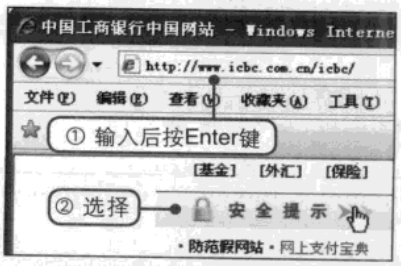
预留验证信息是中国工商银行为了帮助银行有效地识别银行网站、防范不法分子利用假银行网站进行网上诈骗的一项服务。用户在注册中国工商银行个人网上银行的过程中会要求用户必须填写预留信息验证，当用户登录工行个人网上银行、手机银行（WAP）、在购物网站上进行支付或在线签订委托缴费协议时，网页上会自动显示用户预留的信息，以便验证是否为真实的工商银行网站。

8.4.3 使用小e安全检测

小e安全检测是中国工商银行专为网上银行的用户提供的，协助用户在线查杀可能影响网上银行安全的计算机间谍软件。小e安全检测采用国际先进的安全引擎，利用微软Active X技术，通过IE浏览器下载小e安全检测控件和病毒特征码的方式，实现查杀网上银行间谍软件、检测电脑漏洞等功能。

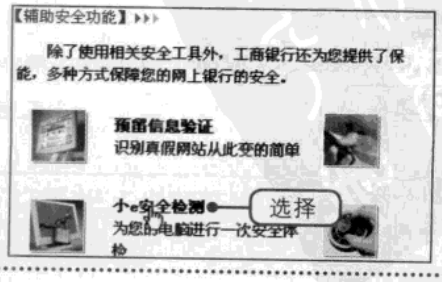
① 选择“安全提示”选项

打开IE浏览器窗口，❶在地址栏中输入www.icbc.com.cn并按Enter键打开工商银行网站。❷选择“安全提示”选项。



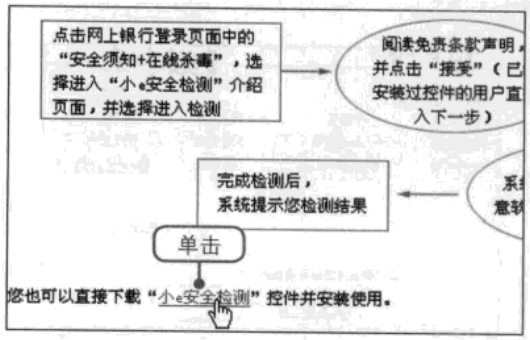
② 选择“小e安全检测”选项

打开新的页面，拖动右侧的滚动条至页面的最下方，接着在页面中选择“小e安全检测”选项。



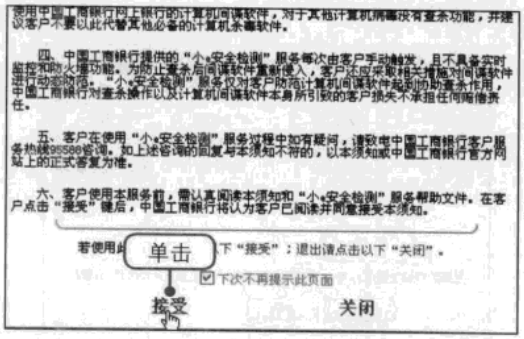
③ 开始安装小e安全检测

打开新的页面，拖动右侧的滚动条，接着单击页面中的“小e安全检测”文字链接。



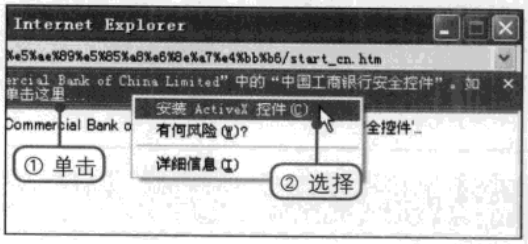
④ 单击“接受”文字链接

切换至新的页面，阅读完相关的信息之后单击下方的“接受”文字链接。



⑤ 选择“安装ActiveX控件”选项

切换至新的界面，①提示用户安装中国工商银行安全控件，单击页面顶部的选项条。②在弹出的菜单中选择“安装ActiveX控件”选项。

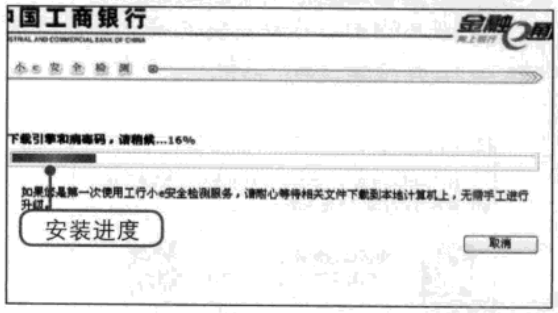


⑥ 开始安装

弹出“Internet Explorer安全警告”提示框，提示用户安装中国工商银行安全控件，单击“安装”按钮。

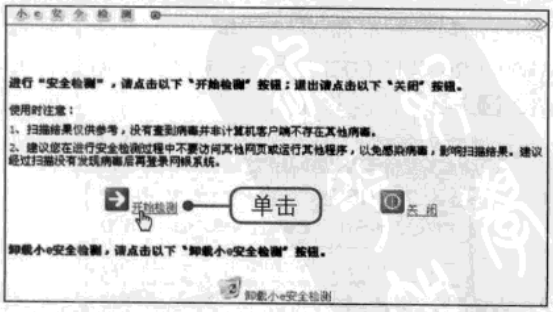
⑦ 查看安装的进度

此时在打开的界面中正在下载引擎和病毒码，可随时查看其下载的进度，请耐心等待。



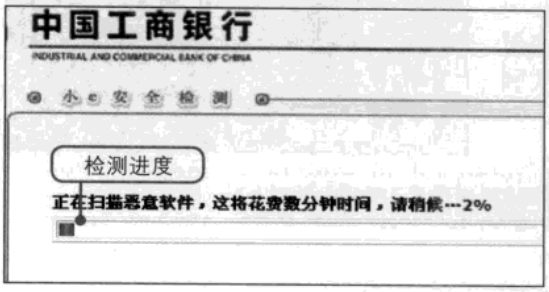
⑧ 开始检测

下载成功后打开新的界面，在界面中单击“开始检测”按钮开始检测系统。



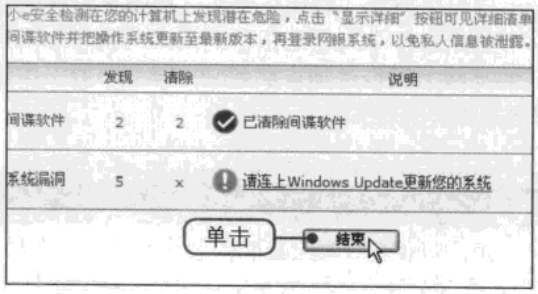
⑨ 设置文件名

在打开的界面中显示小e安全检测正在扫描恶意软件，在页面中可以看见扫描的进度，请耐心等待。



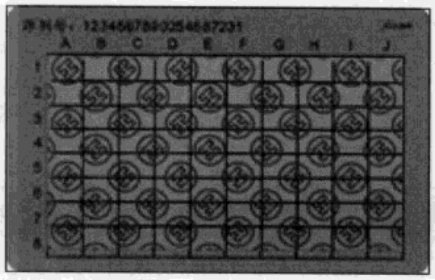
⑩ 检测结束

扫描结束后切换至新的界面，在新的界面中可看见扫描的结果，单击“结束”按钮退出。



8.4.4 使用电子银行口令卡

电子银行口令卡是中国工商银行推出的网上银行安全工具，它是保护客户资金不受损失而设置的又一道防线。



电子口令卡是指以矩阵形式印有若干字符串的卡片，每个字符串对应一个唯一的坐标，当用户使用工商银行电子银行的相关功能时，按系统指定的若干坐标，将卡片上对应的字符串作为密码输入，系统自动校验密码字符的正确性。如果用户已开通个人网上银行，可以携带本人有效身份证件及注册银行卡到工商银行营业厅申请电子银行口令卡。

使用电子银行口令卡会存在卡片丢失或被窥视、拍照、复印等风险。因此用户须保护好自己的口令卡，为了避免口令卡被别人偷窥，建议不要一次刮开所有覆膜。

若用户的电子银行口令卡不慎丢失，可以持有效证件和网上银行注册卡到工商银行营业厅申请新卡，申请新卡的同时旧卡作废。

在领用电子银行口令卡时，需要确认口令卡的包装膜和覆膜是否完好。新申领的口令卡应包含完整的塑料包装膜和覆膜。

8.4.5 使用U盾

U盾是中国工商银行推出并获得国家专利的客户证书USBkey，它为用户提供了办理网上银行业务的高级别安全工具。

U盾是用于网上银行电子签名和数字认证的工具，它内置微型智能卡处理器，采用1024位非对称密钥算法对网上数据进行加密、解密和数字签名，确保网上交易的保密性、真实性、完整性和不可否认性。U盾适用于工商银行网上银行的所有用户，它可以实现交易更安全、支付更方便、功能更全面、服务更多样等功能。

工商银行个人网上银行的用户可携带本人有效身份证件及网上银行注册卡到营业厅申请U盾。申请后安装U盾的操作流程如下。

① 安装U盾驱动程序

用户可使用U盾配套的安装光盘安装U盾驱动程序。

参照工商银行系统设置指南调整计算机设置 → 运行U盾安装光盘 → 选择安装主页面的“系统升级”安装补丁 → 选择安装主页面的“驱动程序安装”开始安装

② 下载信息证书

进入个人网上银行页面下载相关的信息证书。

登录个人网上银行 → 将U盾与电脑主机上的USB接口相连接 → 进入“安全中心—U盾管理—U盾自助下载” → 若不成功，则可前往工商银行营业厅办理

③ 进行对外支付业务操作

下载成功后用户可使用U盾进行对外支付业务操作。

登录个人网上银行 → 办理对外支付业务时，系统提示插入U盾 → 将U盾与计算机主机上的USB接口相连接 → 输入U盾密码并经银行系统验证无误后即可完成操作

为了更安全地使用网上银行，用户需要保护好U盾及密码，确保登录网上银行的电脑安全可靠，定期更新杀毒软件，及时下载补丁程序，不打开来路不明的程序、链接、邮件，保持良好的上网习惯，U盾使用完毕后应及时从电脑上取回。

工行网银助手

工商银行网银助手是工行在现有控件自动化安装软件以及微软相关补丁的基础上开发的一项将所有网银和证书使用的软件以嵌入程序化软件和利用程序去下载的软件。用户可通过工商银行门户网站下载安装。使用其引导功能，可直接完成整个证书驱动、控件以及系统补丁的安装，真正实现一站式的下载安装，便于用户的使用操作。

Chapter 09

阻止病毒入侵电脑

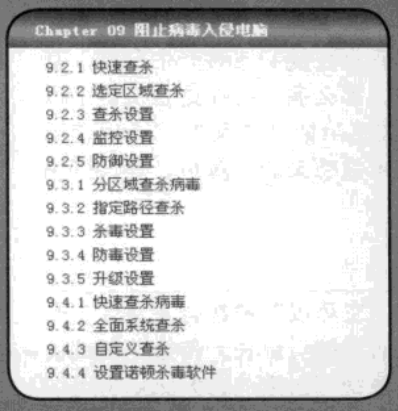
重点知识

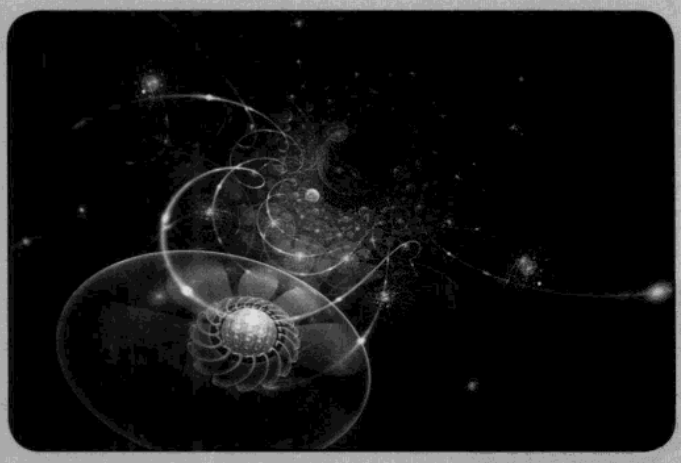
1. 电脑病毒基础知识
2. 使用瑞星杀毒软件查杀病毒
3. 使用金山毒霸杀毒软件查杀病毒
4. 使用诺顿杀毒软件查杀病毒

电脑病毒是指能够破坏电脑功能或数据，并且影响电脑使用的一组计算机指令或者程序代码，它具有自我复制、潜伏等特点。用户在使用电脑的过程中要阻止电脑病毒的入侵，可以使用杀毒软件查杀电脑中潜在的病毒。本章将分别介绍瑞星、金山和诺顿3种杀毒软件。

视频文件

参见随书光盘：视频教程\Chapter 09





9.1 电脑病毒基础知识

打开带有病毒的网站或者下载带有病毒的文件都会使电脑中毒，病毒进入电脑后可在电脑中潜伏一段时间，待条件成熟时便根据程序指令执行更改、删除等破坏电脑的操作，导致用户无法正常使用电脑。

9.1.1 什么是电脑病毒

电脑病毒实质上是一段电脑指令或者程序代码，它们依据程序指令来破坏电脑里的数据和资料，也能附着在各种类型的文件上，当带有病毒的文件从一台电脑复制到另一台电脑时，它们就随着文件而扩散到另一台电脑中。

病毒的产生并不是突发或是偶然的原因。一次突发的停电或者偶然的错误操作会造成计算机的磁盘和内存中产生一些乱码和随机指令，这些代码是无序和混乱的；而病毒则是人为设计的精巧严谨的代码，它按照严格的秩序进行组织，并且与所在的系统网络环境相适应和配合。

9.1.2 电脑病毒的特点

电脑病毒具有以下的特点。

1 寄生性

电脑病毒通常寄生在其他程序之中，当电脑执行这个程序时病毒就产生破坏作用，但是在未启动该程序之前，是不易被发觉的。

2 破坏性

电脑中毒后可能会导致正常的程序无法运行，计算机内的文件被删除或者更改，甚至导致电脑无法正常启动。

3 传染性

病毒不但本身具有破坏性，更可怕的是它还具有传染性，一旦病毒被复制或者产生变种，其速度快的令人难以预防。只要一台电脑感染病毒，如果不及时处理，那么病毒会在这台机器上迅速扩散，其中的大量文件（一般是可执行文件）就会被感染，而被感染的文件又成了新的传染源，这些新的传染源又会通过各种途径从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。

4 潜伏性

一个编制精巧的计算机病毒程序进入电脑后一般不会马上发作，它可以隐藏在合法文件中长达几周、几个月甚至几年。病毒的潜伏性愈好，其在系统中存在的时间就会愈长，传染范围就会愈大。潜伏性的第一种表现是指病毒程序不用专业的检测程序是无法检测出来的，因此病毒可以潜伏在磁盘或者磁盘中很长一段时间，一旦时机成熟就再次四处繁殖、扩散；第二种表现则是指

电脑病毒的内部往往有一种触发机制，在不满足触发条件的情况下病毒仅仅具有传染性，一旦触发条件满足则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、使系统死锁等。

5 隐蔽性

电脑病毒具有很强的隐蔽性，有些病毒可通过查杀病毒软件检查出来，而有些病毒则根本就查不出来，一旦病毒发作，则电脑已经遭受了不小的损失。

9.1.3 电脑病毒的分类

电脑病毒可根据其存在的媒体、传染的方式和破坏的能力进行不同的分类。

1 根据病毒存在的媒体划分

根据电脑病毒存在的媒体可划分为网络病毒、文件病毒和引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件；文件病毒则感染计算机中可执行文件；引导型病毒感染启动扇区（Boot）和硬盘的系统引导扇区（MBR）。

2 根据病毒传染的方法划分

根据电脑病毒传染的方法可划分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后把自身的内存驻留部分放置在内存（RAM）中，驻留在内存中的程序挂接系统调用并合并到操作系统中，它一直处于激活状态，直到关机或重新启动；非驻留型病毒在得到激活的机会时并不在内存驻留具有传染性的程序。

3 根据病毒的破坏能力划分

根据病毒的破坏能力可划分为无害型、无危险型、危险型和非常危险型四类。无害型病毒除了传染时减少磁盘的可用空间外，对系统没有其他影响；无危险型病毒仅仅是占用内存容量、显示图像、发出声音及同类音响；危险型病毒在计算机操作系统中造成严重的错误；非常危险型病毒删除程序、破坏数据、清除系统内存区和操作系统中的重要信息。

9.2 使用瑞星杀毒软件查杀病毒

可以通过在电脑中安装杀毒软件来预防电脑破坏系统，杀毒软件也称反病毒软件，是通过删除病毒、木马和恶意软件来保护电脑安全的一类软件的总称。国产的瑞星杀毒软件是一个不错的选择，用户可登录瑞星官方网站www.rising.com.cn下载瑞星杀毒软件2009。

9.2.1 快速查杀

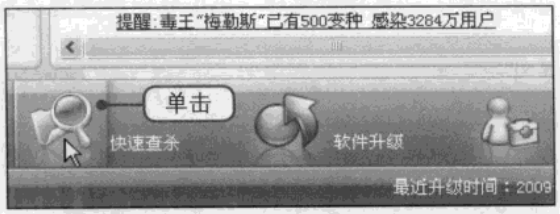
瑞星杀毒软件的快速查杀功能主要是对电脑的硬盘和内存进行快速、全面的扫描。速度较快但是杀毒不全面。

① 启动瑞星杀毒软件

在桌面上双击“瑞星杀毒软件”快捷图标，打开“瑞星杀毒软件”主界面窗口。

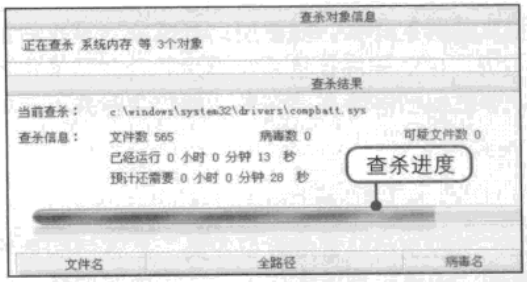
② 单击“快速查杀”按钮

在主界面窗口的底部单击“快速查杀”按钮开始查杀。



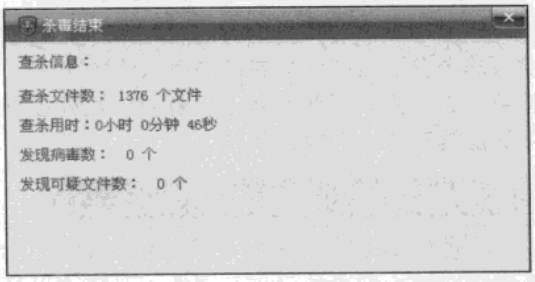
③ 查看查杀病毒的进度

在打开的界面中可以看见查杀病毒的进度，若扫描出病毒则会弹出对话框询问用户怎样处理病毒或带病毒的文件。



④ 杀毒结束

杀毒结束后弹出“杀毒结束”对话框，用户可在对话框中看见查杀的详细信息，接着单击下方的“确定”按钮退出即可。

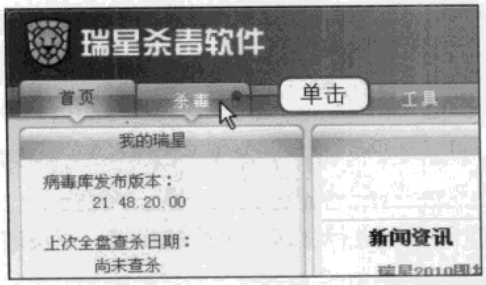


9.2.2 选定区域查杀

瑞星杀毒软件提供的选定区域查杀功能与快速查杀相比查杀速度较慢，但是查杀的范围很广，用户可在查杀病毒之前根据自己的需要选择区域进行查杀。

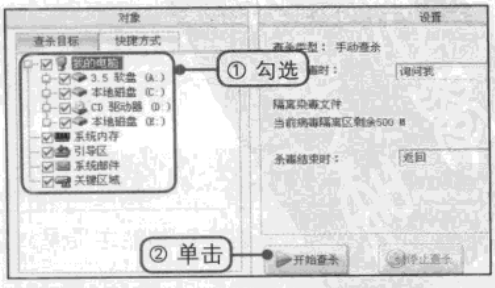
① 单击“杀毒”标签

打开“瑞星杀毒软件”主界面，在窗口中单击“杀毒”标签。



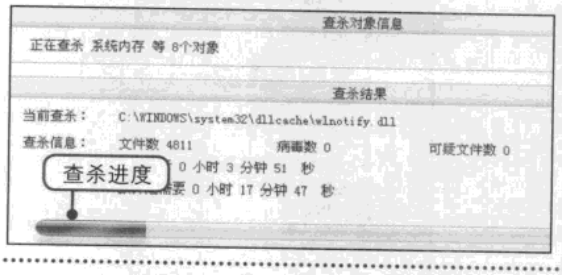
② 选择查杀区域

①在“查杀目标”选项卡下勾选需要查杀区域的复选框。②单击“开始查杀”按钮。



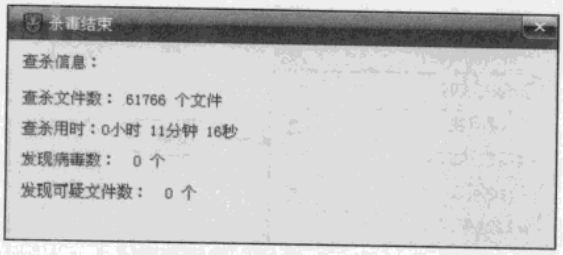
③ 查看查杀病毒的进度

在打开的界面中可以看见查杀病毒的进度，若扫描出病毒则会弹出对话框询问用户怎样处理病毒或带病毒的文件。



④ 杀毒结束

杀毒结束后弹出“杀毒结束”对话框，用户可在对话框中看见查杀的详细信息，接着单击下方的“确定”按钮退出即可。

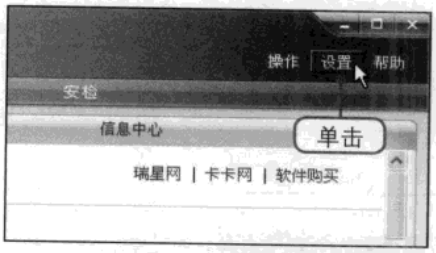


9.2.3 查杀设置

仅仅使用杀毒软件查杀病毒是不够的，还需要对杀毒软件进行相关的设置，首先可在“查杀设置”选项卡中根据自己的实际情况设置手动查杀、空闲时段查杀和开机查杀等选项。

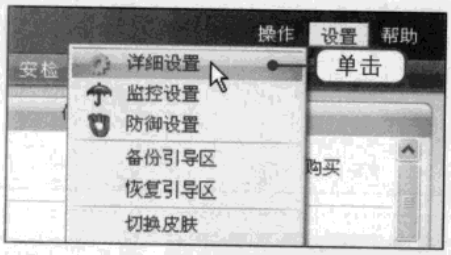
① 单击“设置”按钮

按照前面介绍的方法打开“瑞星杀毒软件”主界面窗口，在窗口的右上方单击“设置”按钮。



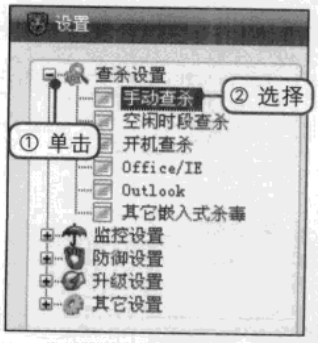
② 打开“设置”对话框

在弹出的菜单中单击“详细设置”命令，打开“设置”对话框。



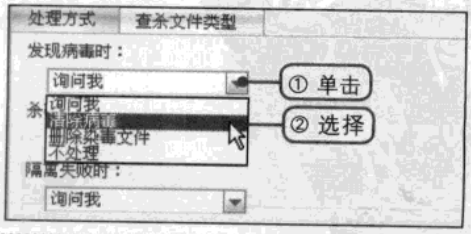
③ 选择“手动查杀”选项

①在“设置”对话框中单击“查杀设置”前的⊞按钮。②在展开的子选项中选择“手动查杀”选项。



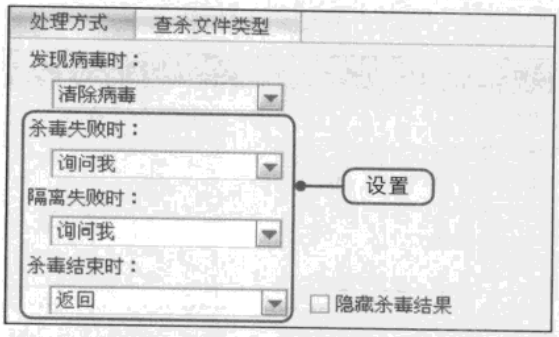
④ 设置发现病毒时的处理方式

①单击“发现病毒时”下拉列表框右侧的下三角按钮。②在弹出的下拉列表中选择“清除病毒”选项。



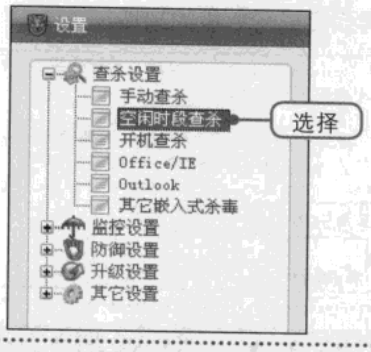
5 设置其他选项

设置“杀毒结束时”、“隔离失败时”和“杀毒结束时”选项。



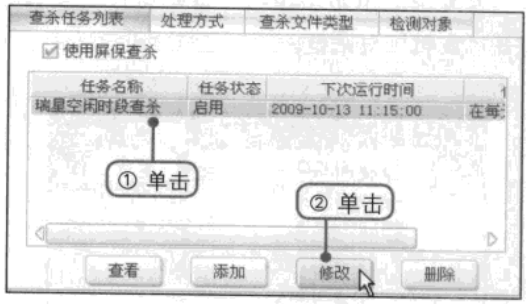
6 选择“空闲时间查杀”选项

设置完毕后选择对话框左侧的“查杀设置选项卡下的“空闲时间查杀”选项。



7 设置查杀任务列表

在对话框右侧的“查杀任务列表”选项卡中设置查杀任务，①单击“瑞星空闲时段查杀”选项。②单击“修改”按钮。

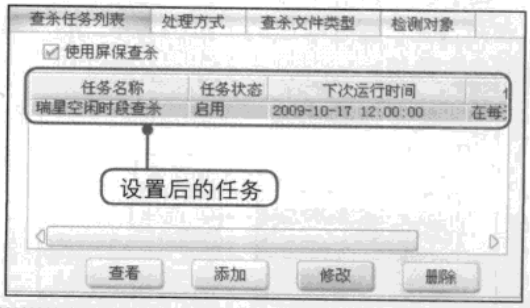


8 打开“修改任务”对话框

弹出“修改任务”对话框，①可根据自身的需要对相关的选项进行设置，例如单击选中“每周末”单选按钮，并且设置开始时间和结束时间。②单击“确定”按钮。

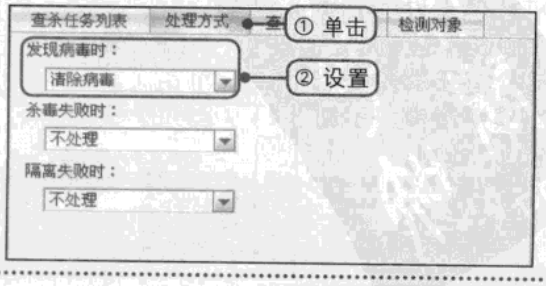
9 查看设置后的任务

返回“设置”对话框，此时可在对话框中看见设置后的任务。



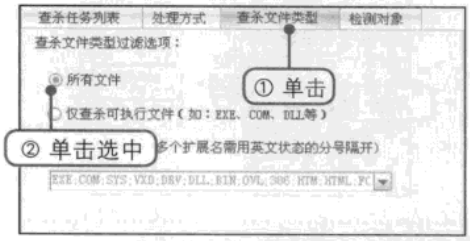
10 设置处理方式

①单击“处理方式”标签切换至该选项卡。②设置发现病毒时的处理方式为清除病毒，其他选项保持默认设置。



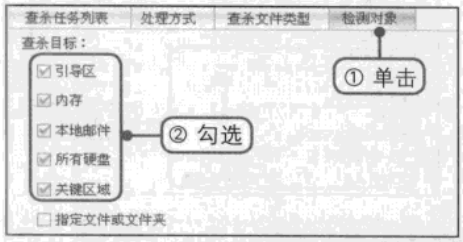
11 设置查杀文件类型

①单击“查杀文件类型”标签切换至该选项卡。②在“查杀文件类型过滤选项”选项组中单击选中“所有文件”单选按钮。



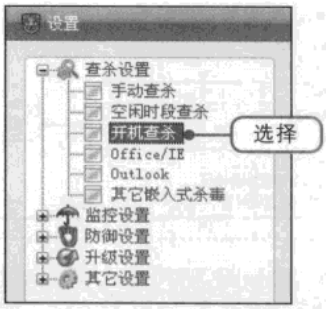
12 设置查杀目标

①单击“检测对象”标签切换至该选项卡。②在“查杀目标”选项组中分别勾选“引导区”、“内存”、“本地邮件”、“所有硬盘”、“关键区域”5个复选框。



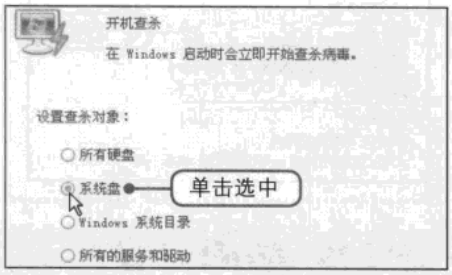
13 选择“开机查杀”选项

在“设置”对话框的左侧选择“查杀设置>开机查杀”选项。



14 设置开机查杀

在对话框右侧的“设置查杀对象”选项组中进行相关设置，例如单击选中“系统盘”单选按钮。

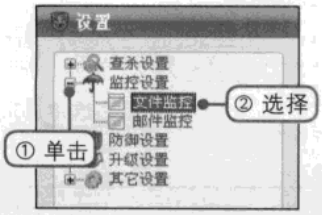


9.2.4 监控设置

可以在“设置”对话框中设置文件监控和邮件监控选项，以便对电脑中重要的文件和电子邮件进行实时保护。

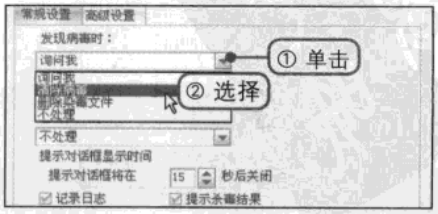
1 选择“文件监控”选项

打开“设置”对话框，①单击“监控设置”选项前的⊞按钮。②在展开的子选项中选择“文件监控”选项。



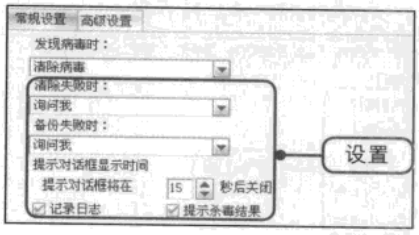
2 常规设置

①在“常规设置”选项卡中单击“发现病毒时”下拉列表框右侧的下三角按钮。②在弹出的下拉列表中选择“清除病毒”选项。



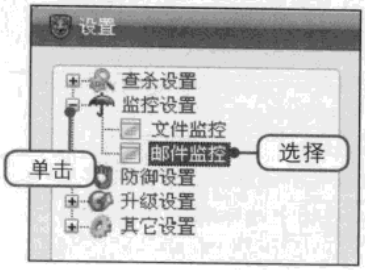
③ 设置其他选项

用户可根据自己的情况设置“清除失败时”、“备份失败时”选项，然后设置提示对话框的显示时间。



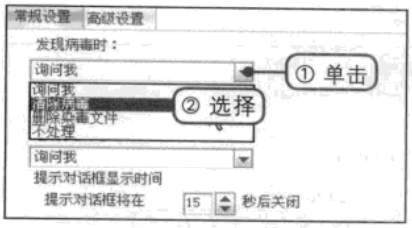
④ 选择“邮件监控”选项

设置完毕后，在对话框的左侧选择“监控设置>邮件监控”选项。



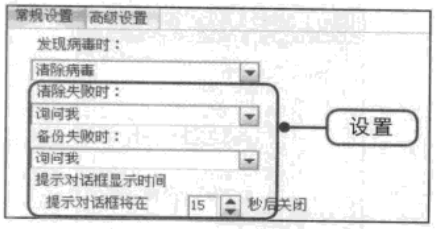
⑤ 常规设置

①在“常规设置”选项卡中单击“发现病毒时”下拉列表框右侧的下三角按钮。②在弹出的下拉列表中选择“清除病毒”选项。



⑥ 设置其他选项

用户可根据自己的情况设置“清除失败时”、“备份失败时”选项，然后设置提示对话框的显示时间。

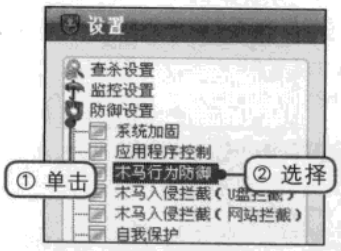


9.2.5 防御设置

可以在防御设置下设置木马行为防御、木马入侵拦截（U盘拦截）和木马入侵拦截（网站拦截）等选项，使电脑在任何时候都能防御入侵。

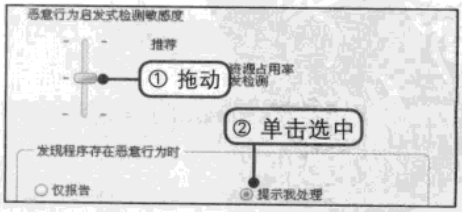
① 选择“木马行为防御”选项

打开“设置”对话框，①单击“防御设置”选项。②在展开的子选项中选择“木马行为防御”选项。



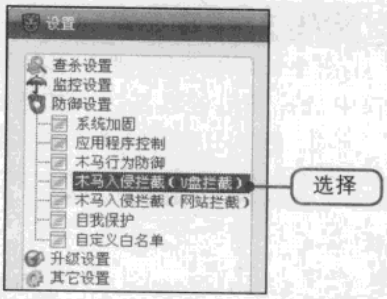
② 设置木马行为防御

①在“恶意行为启发式检测敏感度”选项组中将滑块拖动至中间位置。②在“发现程序存在恶意行为时”选项组中单击选中“提示我处理”单选按钮。



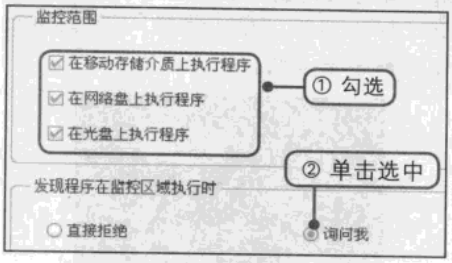
③ 选择 U 盘拦截

在“设置”对话框中选择“防御设置>木马入侵拦截（U盘拦截）”选项。



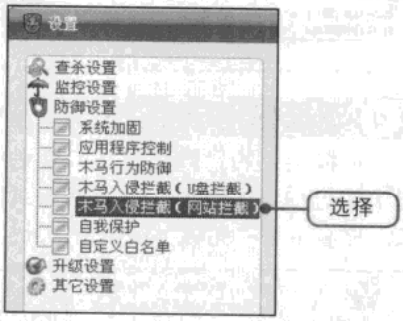
④ 设置木马入侵拦截（U盘拦截）

①在“监控范围”选项组中勾选所有的复选框。②在“发现程序在监控区域执行时”选项组中单击选中“询问我”单选按钮。



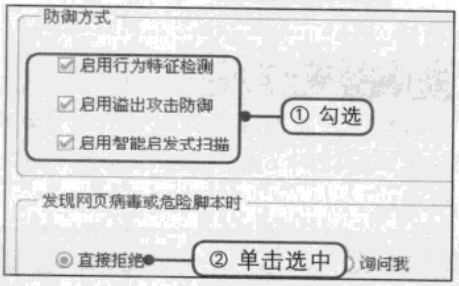
⑤ 选择网站拦截

在“设置”对话框中选择“防御设置>木马入侵拦截（网站拦截）”选项。



⑥ 设置木马入侵拦截（网站拦截）

①在“防御方式”选项组中勾选所有的复选框。②在“发现网页病毒或危险脚本时”选项组中单击选中“直接拒绝”单选按钮。



9.3 使用金山毒霸杀毒软件查杀病毒

金山毒霸（King soft Anti-Virus）是国内比较出名的一款反病毒软件，它融合了代码分析、虚拟机查毒等成熟可靠的反病毒技术，使该软件在查杀病毒种类和速度以及未知病毒防治等多方面具有明显的优势。同时，金山毒霸具有病毒防火墙实时控制、压缩文件查毒、查杀电子邮件病毒等多项先进的功能。

9.3.1 分区域查杀病毒

可以登录金山毒霸官方网站www.duba.net下载金山毒霸杀毒软件，下载后将杀毒软件安装至

电脑后就可执行查杀病毒操作。查杀方式包括“分区域查杀”和“‘指定路径’查杀”两种，其中分区域查杀是指在金山2009杀毒软件主界面下选择要查杀病毒的区域后对所选择的范围比较大的区域进行扫描。

① 启动金山毒霸杀毒软件

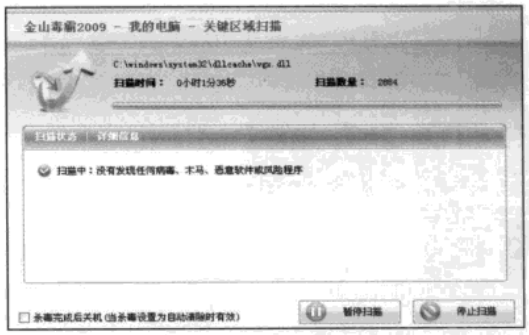
在桌面上双击“金山毒霸”快捷图标，启动金山毒霸杀毒软件。

② 选择扫描的区域

打开金山毒霸杀毒软件的主界面窗口，①在窗口中选择扫描的区域，例如选择“我的电脑”选项。②单击右侧的“开始扫描”按钮。

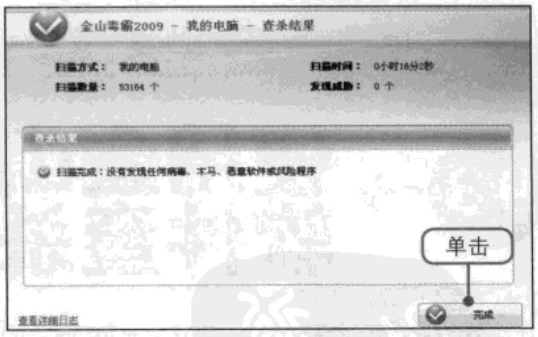
③ 扫描病毒

杀毒软件开始扫描计算机中的恶意软件，扫描结束后开始对“我的电脑”进行扫描，请耐心等待。



④ 查看扫描结果

扫描结束后，用户可在“查杀结果”选项组中看见扫描的结果，若有病毒可手动将其查杀。接着单击“完成”按钮退出即可。

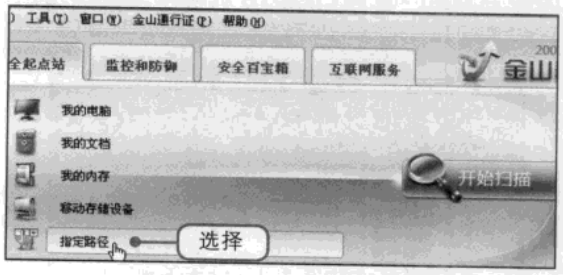


9.3.2 指定路径查杀

当用户已估计出病毒可能存在于某个磁盘分区内时，可以选择“指定路径”查杀病毒。

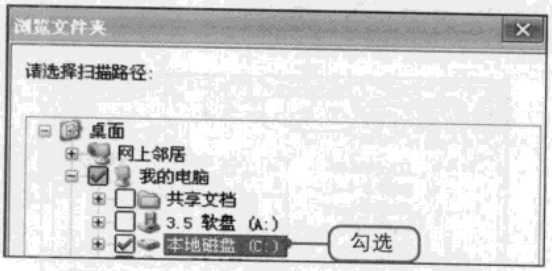
① 选择“指定路径”选项

打开金山毒霸杀毒软件主界面窗口，选择“指定路径”选项。



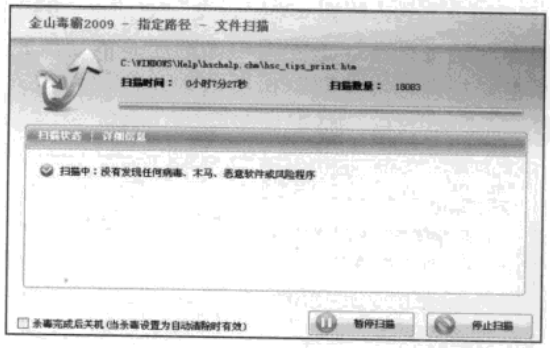
② 选择扫描路径

弹出“浏览文件夹”对话框，在“请选择扫描路径”下方勾选“本地磁盘(C:)”复选框。



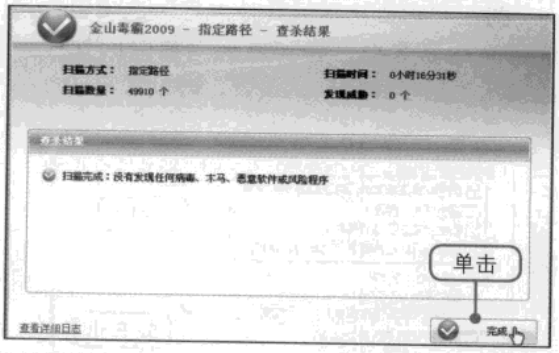
③ 开始扫描

返回主界面窗口，杀毒软件开始扫描恶意软件，结束后开始扫描C盘，请耐心等待。



④ 查看扫描结果

若扫描出病毒则可手动将其清除。清除完毕后单击“完成”按钮退出即可。



使用金山毒霸进行在线杀毒

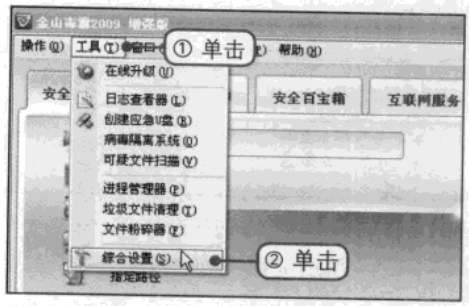
除了将杀毒软件安装至电脑中之外，还可以登录金山毒霸官方网站使用在线杀毒。在线杀毒随时更新病毒库而且提供免费查杀病毒，另外，还可以使用该功能为电脑修复系统漏洞。

9.3.3 杀毒设置

金山杀毒软件同样为用户提供了综合设置，包括杀毒设置、防毒设置和升级设置等，从而使金山毒霸杀毒软件能更好地配合用户保护电脑。用户可在杀毒设置中分别按照自己的需求设置手动杀毒、屏保杀毒和定时杀毒。

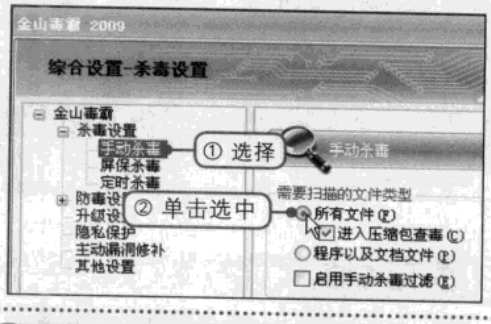
① 单击“综合设置”命令

打开金山毒霸杀毒软件主界面窗口，①单击菜单栏中的“工具”标签。②在弹出的菜单中单击“综合设置”命令。



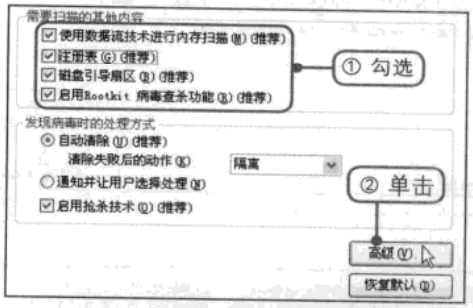
② 设置需要扫描的文件类型

弹出“综合设置—杀毒设置”对话框，①在左侧选择“杀毒设置>手动杀毒”选项。②在对话框右侧的“需要扫描的文件类型”选项组中单击选中“所有文件”单选按钮。



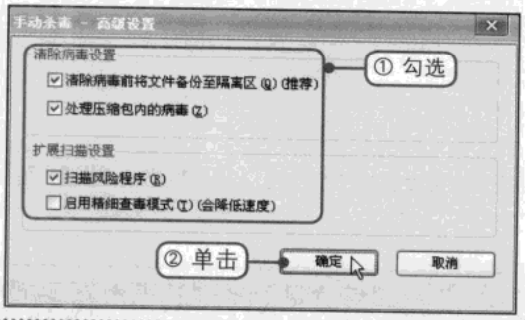
③ 设置需要扫描的其他内容

①在“需要扫描的其他内容”选项组中勾选所有的复选框，在“发现病毒时的处理方式”选项组中保持默认设置。②设置完毕后单击“高级”按钮。



④ 手动杀毒高级设置

弹出“手动杀毒—高级设置”对话框，①在“清除病毒设置”选项组中勾选所有的复选框并在“扩展扫描设置”选项组中勾选“扫描风险程序”复选框。②单击“确定”按钮。

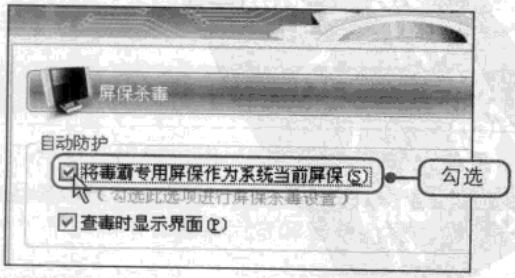


⑤ 选择“屏保杀毒”选项

返回“综合设置—杀毒设置”对话框，选择对话框左侧的“屏保杀毒”选项。

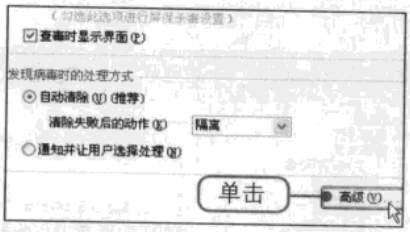
⑥ 设置屏保杀毒

在对话框右侧的“自动防护”选项组下勾选“将毒霸专用屏保作为系统当前屏保”复选框。



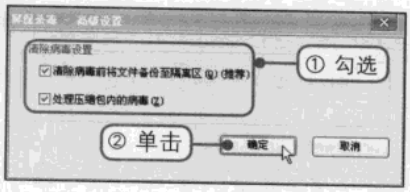
⑦ 单击“高级”按钮

保持“发现病毒时的处理方式”选项组中的设置，直接单击下方的“高级”按钮。



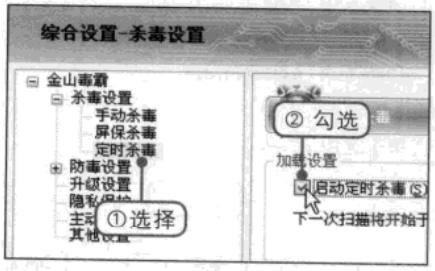
⑧ 屏保杀毒高级设置

打开“屏保杀毒—高级设置”对话框，①在“清除病毒设置”选项组中勾选所有复选框。②单击“确定”按钮。



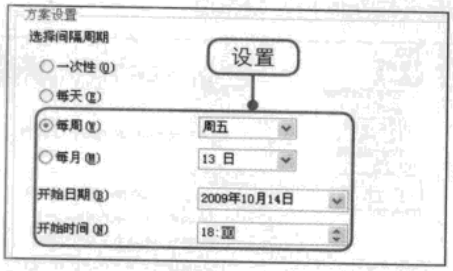
⑨ 选择“定时杀毒”选项

返回“综合设置—杀毒设置”对话框，①选择左侧的“定时杀毒”选项。②在对话框的右侧勾选“启动定时杀毒”复选框。



⑩ 设置定时杀毒方案

在“方案设置”选项组中设置间隔周期，例如单击选中“每周”单选按钮并在右侧选择“周五”选项。接着设置开始日期和时间。

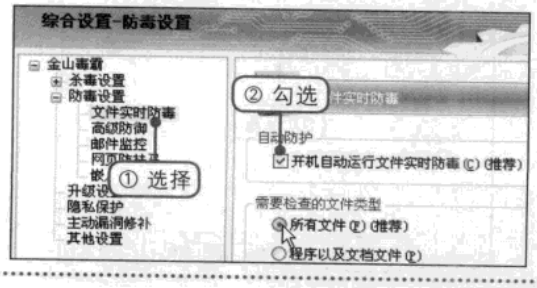


9.3.4 防毒设置

可在防毒设置中设置文件实时防毒、高级防御和邮件监控等选项，使电脑时刻处于防御病毒的最佳状态。

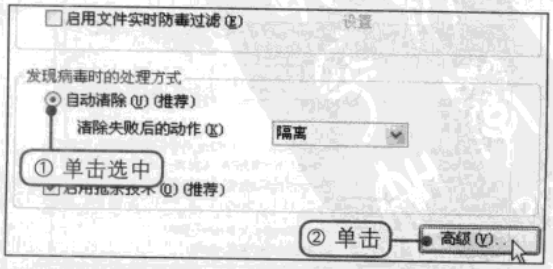
① 选择“文件实时防毒”选项

①在对话框左侧选择“防毒设置>文件实时防毒”选项。②在右侧勾选“开机自动运行文件实时防毒”复选框。



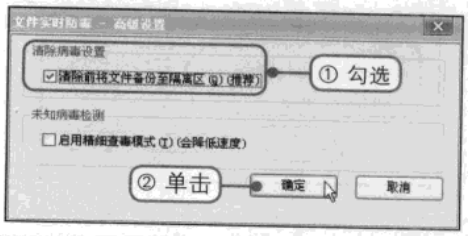
② 设置文件实时防毒

①在“发现病毒时的处理方式”选项组中单击选中“自动清除”单选按钮。②单击“高级”按钮。



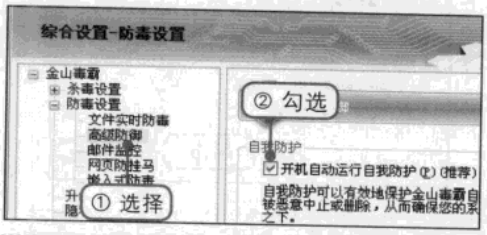
③ 文件实时防毒高级设置

打开“文件实时防毒—高级设置”对话框，①勾选“清除前将文件备份至隔离区”复选框。②单击“确定”按钮。



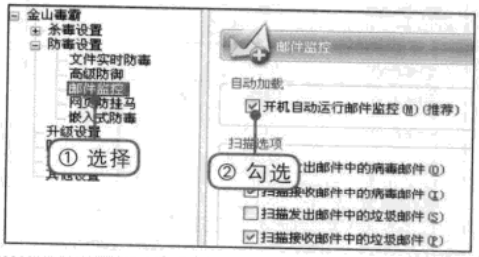
④ 设置高级防御

返回“综合设置—防毒设置”对话框，①选择对话框左侧的“高级防御”选项。②在右侧勾选“开机自动运行自我防护”复选框。



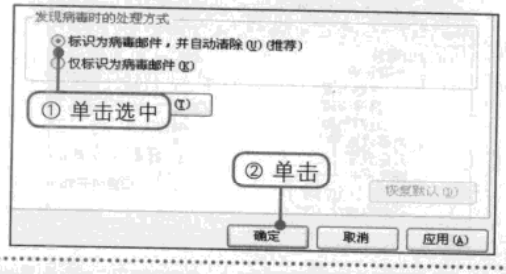
⑤ 选择“邮件监控”选项

①选择对话框左侧的“邮件监控”选项。②在右侧勾选“自动加载”选项组中的“开机自动运行邮件监控”复选框。



⑥ 单击“反垃圾邮件设置”按钮

①在“发现病毒时的处理方式”选项组中单击选中“标识为病毒邮件，并自动清除”单选按钮。②单击“确定”按钮。

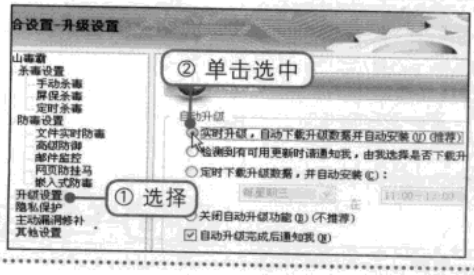


9.3.5 升级设置

可在升级设置选项中设置自动升级的方式、系统繁忙时自动升级的处理情况和选择是否使用代理服务器。

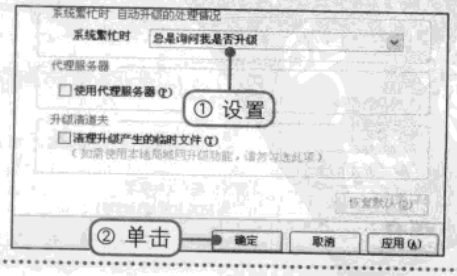
① 选择“升级设置”选项

①在对话框的左侧选择“升级设置”选项。②在右侧单击选中“实时升级，自动下载升级数据并自动安装”单选按钮。



② 升级设置

①在“系统繁忙时自动升级的处理情况”选项组中设置系统繁忙时为“总是询问我是否升级”。②最后单击“确定”按钮保存退出。



9.4 使用诺顿杀毒软件查杀病毒

诺顿杀毒软件是Symantec公司个人信息安全产品之一，也是一个被广泛应用的反病毒程序。它不仅能够严密防范黑客、病毒、木马、间谍软件和蠕虫等的攻击，全面保护用户的信息资产，而且在查杀过程中可以对未知病毒实现“捕获、分析、升级”的智能化分析过程。

9.4.1 快速查杀病毒

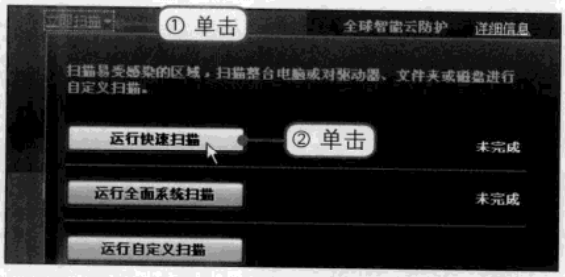
诺顿杀毒软件查杀病毒的方式有快速扫描、全面系统扫描和自定义扫描三种。快速扫描主要是扫描系统中容易遭受病毒感染的区域和启动文件等选项，速度很快。

① 启动诺顿杀毒软件

将诺顿杀毒软件安装至电脑中后，双击桌面上对应的快捷图标，打开其主界面窗口。

② 单击“运行快速扫描”按钮

①单击窗口中的“立即扫描”选项。②在弹出的列表框中单击“运行快速扫描”按钮。

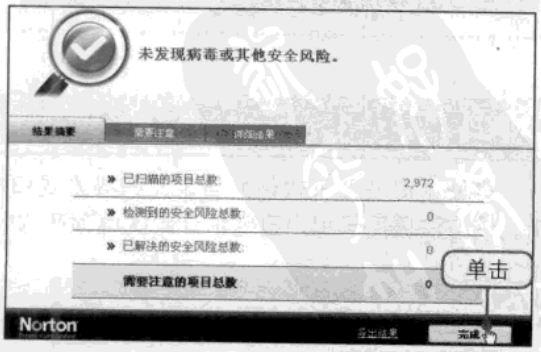


③ 开始扫描

弹出“诺顿快速扫描”对话框，软件开始对系统中容易遭受病毒感染的区域和启动文件等进行扫描，请耐心等待。

④ 查看扫描结果

扫描完毕后用户可在对话框中查看扫描的结果，若扫描出病毒则可手动查杀。清除完毕后单击“完成”按钮。

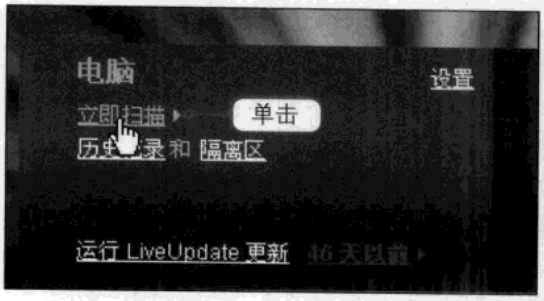


9.4.2 全面系统查杀

诺顿杀毒软件的全面系统扫描方式是针对电脑中的内存和所有磁盘等设备进行仔细地扫描，速度比较慢。

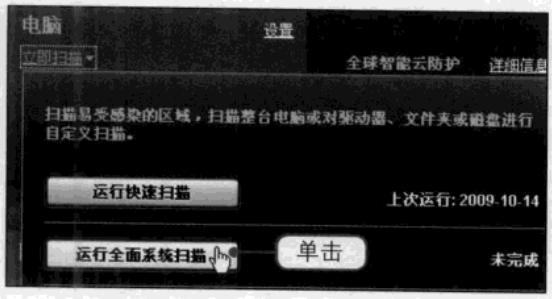
① 单击“立即扫描”选项

打开诺顿杀毒软件主界面，在窗口中单击“立即扫描”选项。



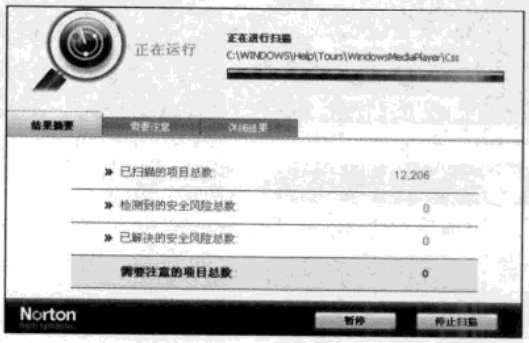
② 单击“运行全面系统扫描”按钮

在弹出的列表框中单击“运行全面系统扫描”按钮。



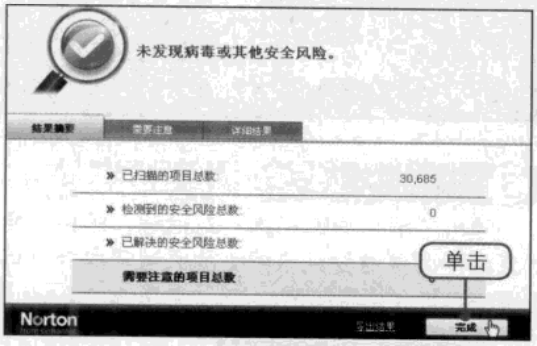
③ 开始扫描

弹出“全面系统扫描”对话框，杀毒软件开始对系统进行全面的扫描，请耐心等待。



④ 查看扫描结果

扫描结束后可在对话框中看见扫描的结果，清除病毒后单击“完成”按钮退出即可。

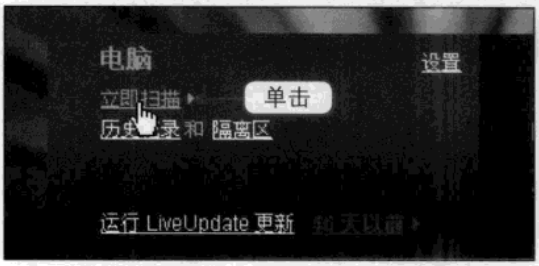


9.4.3 自定义查杀

可使用诺顿杀毒软件的自定义扫描方式扫描电脑中的磁盘分区、文件夹或者文件中的任意一个。该方法适用于用户已经估计到病毒存在的大概位置，速度较快。

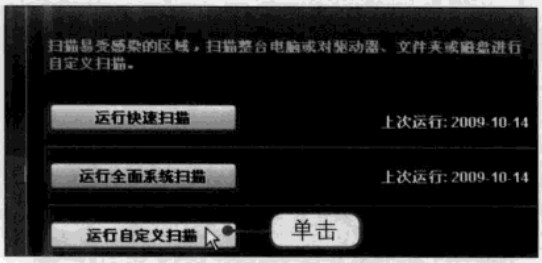
① 单击“立即扫描”选项

打开诺顿杀毒软件主界面窗口，在窗口中单击“立即扫描”选项。



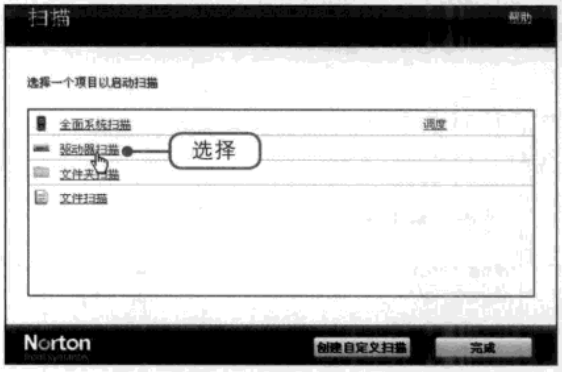
② 单击“运行自定义扫描”按钮

在弹出的列表框中单击“运行自定义扫描”按钮。



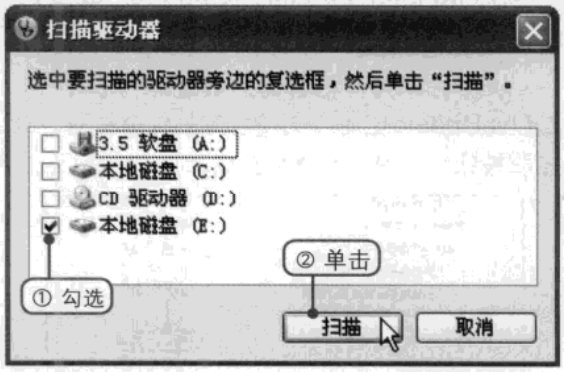
③ 选择扫描项目

弹出“扫描”对话框，在下方的列表框中选择“驱动器扫描”选项。



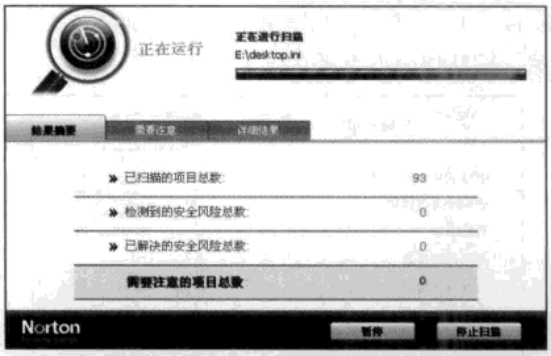
④ 选择扫描的驱动器

弹出“扫描驱动器”对话框，①勾选“本地磁盘(E：)”复选框。②单击“扫描”按钮。



⑤ 开始扫描

弹出“驱动器扫描”对话框，杀毒软件开始对选中的驱动器进行扫描，请耐心等待。



⑥ 查看扫描结果

扫描结束后可在对话框中看见扫描的结果，清除病毒后单击“完成”按钮退出即可。

9.4.4 设置诺顿杀毒软件

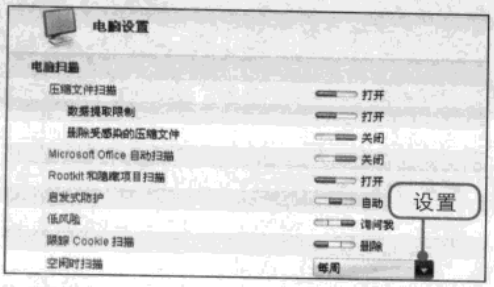
诺顿杀毒软件的设置包括电脑设置、网络设置和其他设置。用户可根据自己的情况参照下面的步骤进行设置。

① 单击“设置”文字链接

打开诺顿杀毒软件主界面，在窗口中单击“设置”文字链接。

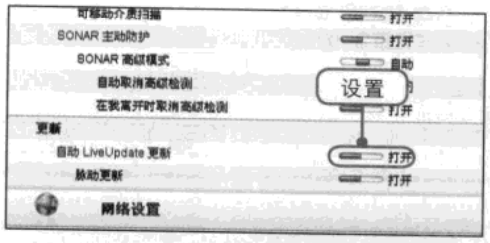
② 电脑设置

打开“设置”对话框，在“电脑设置”选项卡下设置空闲时扫描为每周。



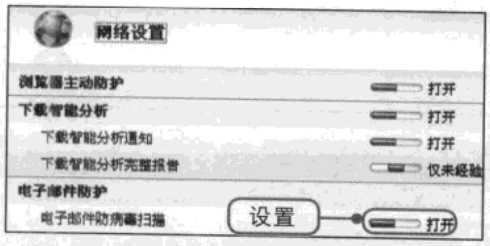
③ 开启自动LiveUpdate更新

向下拖动对话框右侧的滚动条，单击“自动LiveUpdate更新”选项右侧的红色按钮，单击后按钮呈现绿色并滑至左侧。



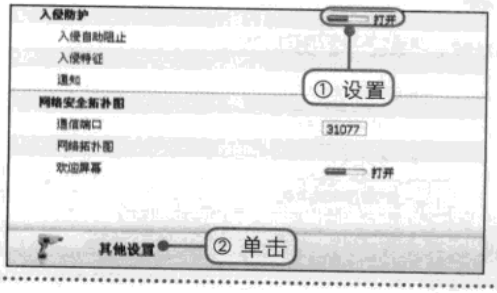
④ 开启电子邮件防护

单击“网络设置”选项切换至该选项卡下，按照步骤3的方法设置电子邮件防病毒扫描为打开状态。



⑤ 开启入侵防护

向下拖动对话框右侧的滚动条，①同样的方法设置入侵防护为打开状态。②单击下方的“其他设置”选项。



⑥ 查看扫描结果

在“其他设置”选项卡下设置空闲时优化程序为打开状态。接着单击对话框底部的“确定”按钮保存退出即可。

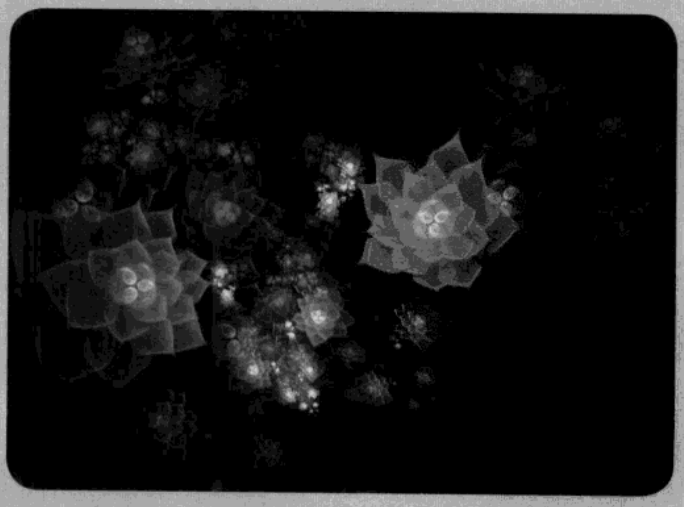
Chapter 10

了解黑客

重点知识

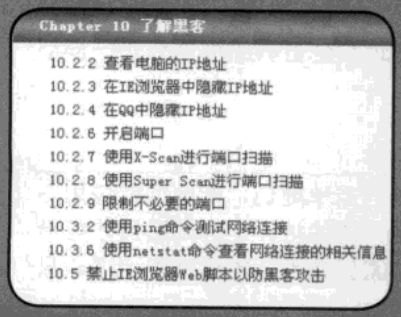
1. 什么是黑客
2. 黑客进入电脑的通道——IP和端口
3. 黑客常用的命令
4. 黑客常使用的入侵手段
5. 禁止IE浏览器Web脚本以防黑客攻击

黑客是一类喜欢用智力通过创造性的方法来挑战脑力极限的人，在早期的电脑界是带有褒义的，但是到了今天，黑客却是指那些专门利用电脑网络搞破坏或者恶作剧的人。黑客是通过获取他人的电脑IP地址并通过端口入侵电脑的，如果用户了解了黑客的入侵方法、常用工具和命令，可在一定程度上防止黑客入侵到自己的电脑中。



视频文件

参见随书光盘：视频教程\Chapter 10



10.1 什么是黑客

“黑客”是英文hacker直接音译而来的，可将黑客简单地理解为破坏者，黑客一般都是利用系统或者软件的漏洞来入侵电脑的，如果用户使用了一些较为危险的操作同样会给黑客创造机会，通俗地说，黑客最拿手的就是乘人之危。

黑客一词，原意是指计算机技术水平超高的电脑专家，尤其是指程序设计人员。但到了今天，黑客一词已被用于泛指那些专门利用电脑网络搞破坏或恶作剧的家伙，而对这些人正确的英文叫法是cracker，音译为“骇客”。黑客与骇客的主要区别是黑客们修补相关漏洞，而骇客们却抓住这些漏洞对其他电脑进行入侵。

黑客是指那些精通操作系统和网络技术，并善于利用专长编制新程序的人，他们一般都掌握着非凡的计算机技术和网络知识，他们可通过别人的电脑来盗取其他计算机内的重要文件，造成别人电脑的系统崩溃、磁盘格式化、监听别人电脑或者偷窥他人隐私，远程控制他人计算机等。

10.2 黑客进入电脑的通道——IP和端口

黑客要入侵别人的电脑，首先需要获取目标电脑的IP地址，然后再通过该电脑上的端口来发动攻击。IP地址是Internet给每个连接在Internet上的主机分配的一个32位地址，它就像是用户的家庭住址一样；而端口则是电脑与外界通信交流的出口。

10.2.1 IP和IP地址

1 IP

IP是英文Internet Protocol的缩写，中文意思是网络之间互连的协议，它是用来唯一标识互联网上计算机的逻辑地址。每台接入互联网的计算机都是依靠IP地址来标识自己的，类似于用户的电话号码，只有通过电话号码才可找到对应用户的实际地址。IP地址与全世界的电话号码一样都是唯一的。

2 IP地址

IP地址是给每一台连接在互联网上的主机分配的一个32位地址。简单地说，IP地址就像用户的家庭住址一样，如果要写信给另外一个人，则必须要知道他（她）的住址，这样邮递员才能准确地把信送到，电脑发送信息就像是邮递员，它必须知道唯一的“家庭住址”才能准确传送，只不过用户的地址是用文字来表示，而电脑的地址则是用十进制数字表示。

IP地址根据自身的结构可分为A、B、C、D、E五类。

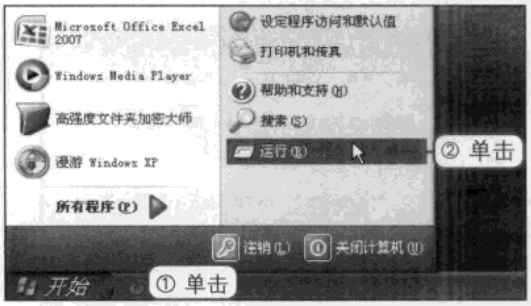
- A类地址用于政府机构，其地址范围为1.0.0.1~126.255.255.254，另外127.X.X.X是保留地址，用做循环测试。
- B类地址用于中等规模公司，其地址范围为128.0.0.1~191.255.255.254。
- C类地址用于任何需要的用户，其地址范围为192.0.0.1~223.255.255.254，另外192.168.0.0~192.168.255.255是私有地址。
- D类地址用于组播，其地址范围为224.0.0.1~239.255.255.254。
- E类地址用于实验，其地址范围为240.0.0.1~255.255.255.254。

10.2.2 查看电脑的IP地址

用户若想查看自己电脑的IP地址，可在命令提示符中使用ipconfig命令查看。如果使用路由器上网，细心的用户会发现每次使用该指令查看的IP地址都不一样，其实这是由于用户使用路由器后，路由器是随机地为电脑分配一个上网的IP地址的。若使用的不是路由器而是MODEM，则使用该指令查看的IP地址就是该电脑在互联网中的IP地址。

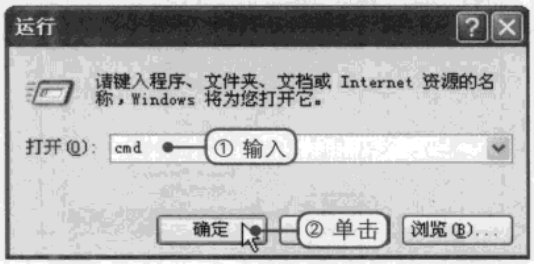
① 打开“运行”对话框

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“运行”命令，打开“运行”对话框。



② 打开命令提示符

①在“打开”文本框中输入cmd命令。②单击“确定”按钮后打开命令提示符。



③ 输入ipconfig命令

在命令提示符中输入ipconfig命令后按Enter键。

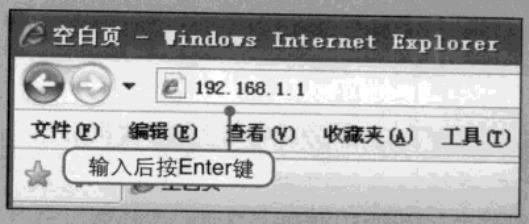
④ 查看IP地址

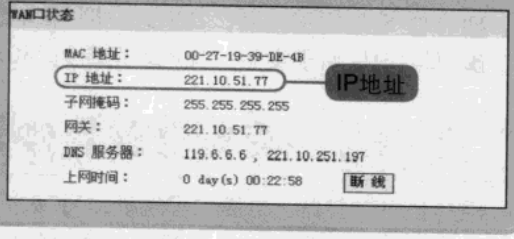
此时可在命令提示符中看见电脑对应的IP地址，例如本机的IP地址为192.168.1.115。

在使用路由器上网的电脑中查看其真实的IP地址

提示

使用路由器的用户可在IE浏览器窗口中输入192.168.1.1后按Enter键，接着在弹出的对话框中输入正确的用户名和密码打开路由器设置界面，此时用户可在“WAN口状态”选项组中看见IP地址，该地址便是用户上网时电脑的真实IP地址。



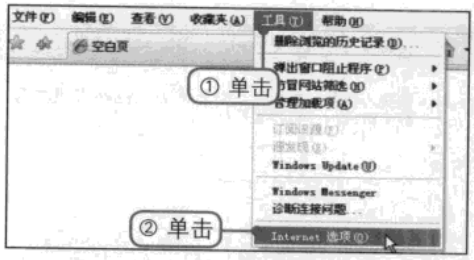


10.2.3 在IE浏览器中隐藏IP地址

在使用IE浏览器打开网页时，若想隐藏电脑的IP地址则可在“Internet选项”对话框中设置使用代理服务器。

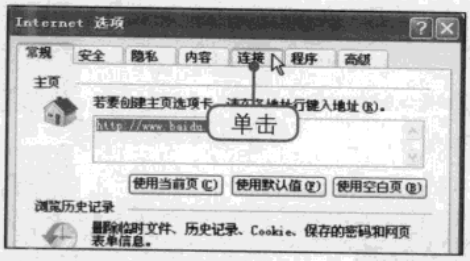
① 单击“Internet选项”命令

①单击IE窗口中的“工具”选项。②在弹出的菜单中单击“Internet选项”命令。



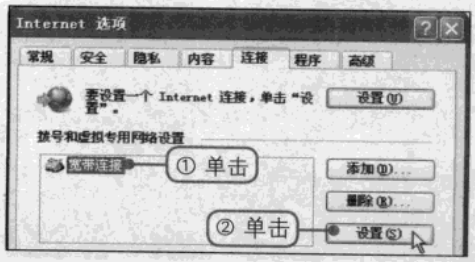
② 切换至“连接”选项卡

弹出“Internet选项”对话框，单击“连接”标签切换至该选项卡。



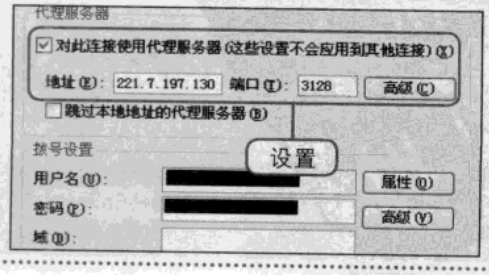
③ 单击“设置”按钮

①在“拨号和虚拟专用网络设置”选项组中单击“宽带连接”选项。②单击右侧的“设置”按钮。



④ 设置代理服务器

弹出“宽带连接设置”对话框，勾选“对此连接使用代理服务器”复选框并输入地址和端口，接着单击“确定”按钮保存退出。

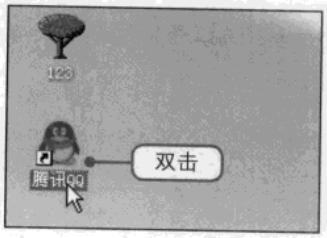


10.2.4 在QQ中隐藏IP地址

若担心使用QQ时泄露电脑的IP地址，则可通过设置代理服务器来隐藏IP地址。

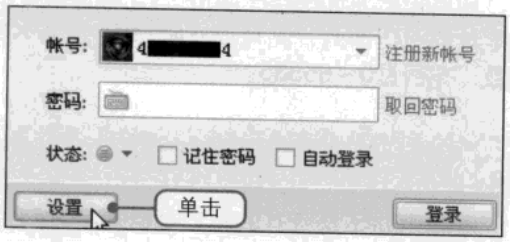
① 启动QQ应用程序

在桌面上双击“腾讯QQ”快捷图标，启动QQ应用程序。



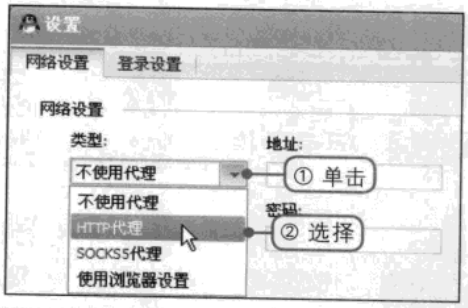
② 单击“设置”按钮

打开QQ登录窗口，单击下方的“设置”按钮。



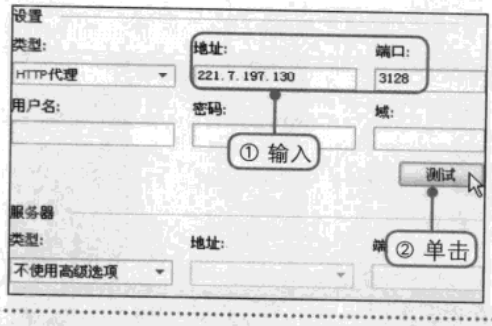
③ 选择使用HTTP代理

弹出“设置”对话框，①单击“类型”下拉列表框右侧的下三角按钮。②在弹出的下拉列表中选择“HTTP代理”选项。



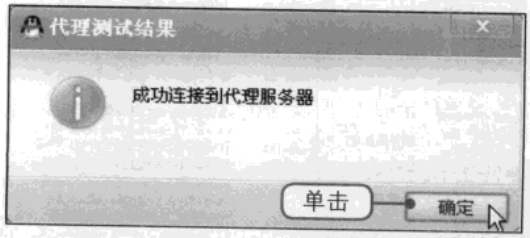
④ 测试代理服务器

①在“设置”对话框右侧的“地址”和“端口”文本框中输入代理服务器的地址和端口。②单击“测试”按钮。



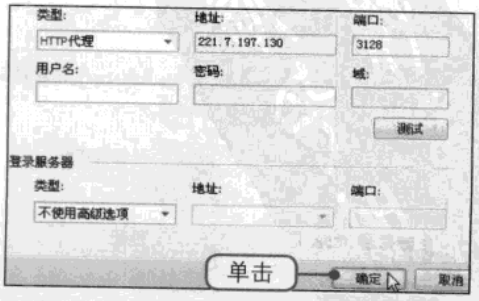
⑤ 连接成功

弹出“代理测试结果”提示框，提示用户成功连接到代理服务器，单击“确定”按钮。



⑥ 保存退出

返回“设置”对话框，直接单击下方的“确定”按钮保存退出即可。



10.2.5 端口概述

端口（port）是计算机与外界通信交流的出口，其中，硬件领域的端口又称接口，如USB端口、串行端口等；而软件领域的端口包括一些数据结构和I/O（基本输入输出）缓冲区。在网络技术中，端口有多种意思，集线器、交换机、路由器的端口是指连接其他网络设备的接口，如RJ-45端口、Serial端口等。而这里所指的端口不是指物理意义上的端口，而是特指TCP/IP协议中的端口，即逻辑意义上的端口。

如果把IP地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，而一个IP地址的门，即端口则可以有65536（256×256）个。端口是通过端口号来标记的，端口号只有整数，范围是0～65535。

10.2.6 开启端口

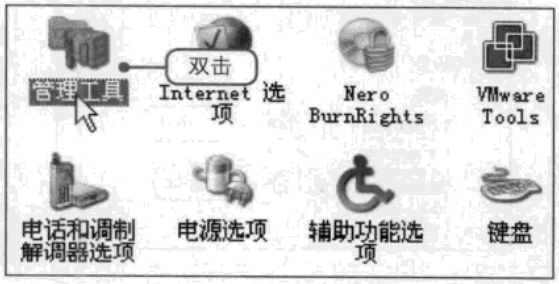
电脑中并不是所有的端口都会被黑客利用，端口号靠前的一些端口是安全的，而这些端口对于电脑的性能发挥着一定的作用，因此用户可手动开启这些端口，开启端口就是在“服务”窗口中启动对应的服务。

① 单击“控制面板”命令

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“控制面板”命令。

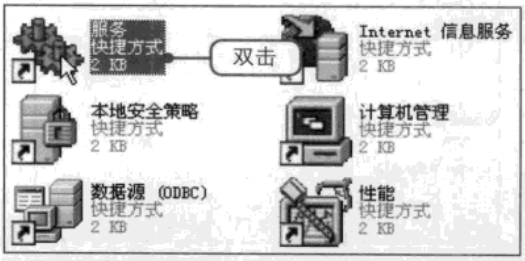
② 双击“管理工具”命令

打开“控制面板”窗口，在窗口中双击“管理工具”快捷图标。



③ 打开“服务”窗口

打开“管理工具”窗口，在窗口中双击“服务”快捷图标，打开“服务”窗口。

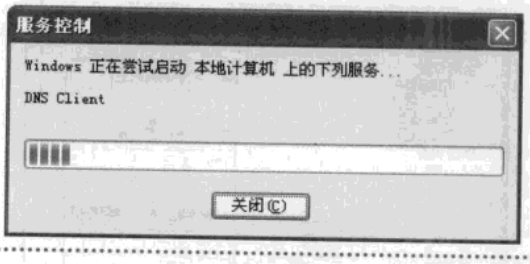


④ 单击“启动”命令

①在“服务”窗口中右击需要开启的服务。②在弹出的快捷菜单中单击“启动”命令。

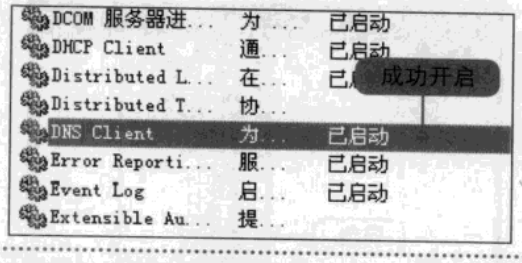
⑤ 启动该服务

弹出“服务控制”对话框，Windows正在尝试启动本地计算机上的DNS Client服务。片刻之后即可启动。



⑥ 成功开启

返回“服务”窗口，可在窗口中看见DNS Client服务已经成功启动。

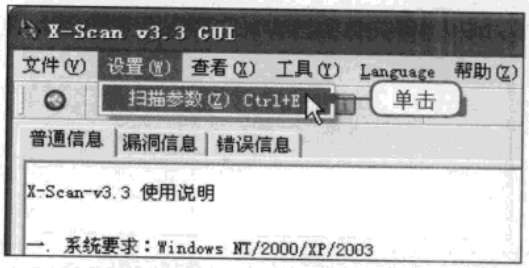


10.2.7 使用X-Scan进行端口扫描

X—Scan是国内著名的综合扫描器之一，是完全免费的，并且不需要安装即可直接使用。用户在使用X—Scan进行端口扫描之前需设置相关的扫描参数。

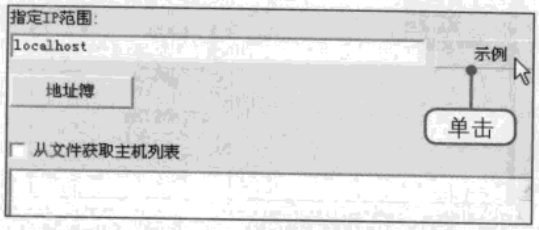
① 单击“扫描参数”命令

启动X—Scan，在其主界面窗口中单击菜单栏中的“设置>扫描参数”命令。



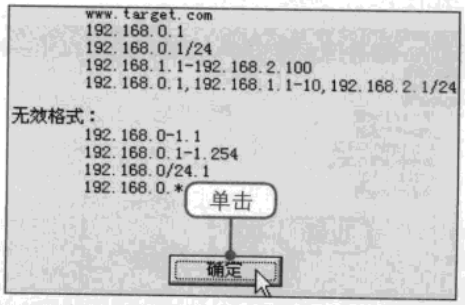
② 单击“示例”按钮

打开“扫描参数”对话框，在左侧选择“检测范围”选项，然后单击“指定IP范围”文本框右侧的“示例”按钮。



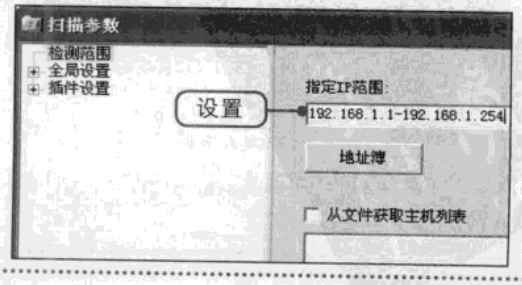
③ 查看示例格式

弹出“示例”对话框，在对话框中查看有效的示例格式后单击“确定”按钮。



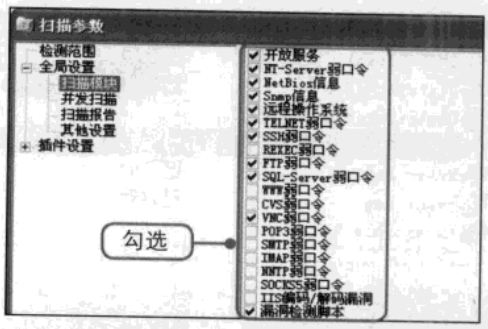
④ 指定IP范围

返回“扫描参数”对话框，根据前面的示例设置IP范围，例如设置IP范围为192.168.1.1-192.168.1.254。



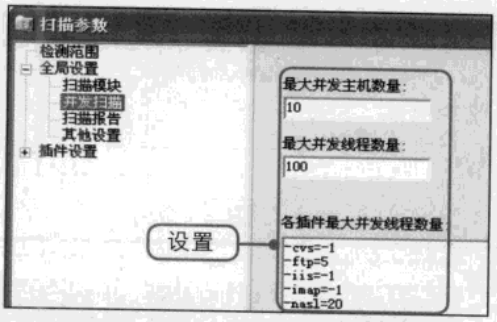
⑤ 设置扫描模块

展开“全局设置>扫描模块”目录树，勾选本次扫描需要加载的插件，这些插件就是要扫描的内容。



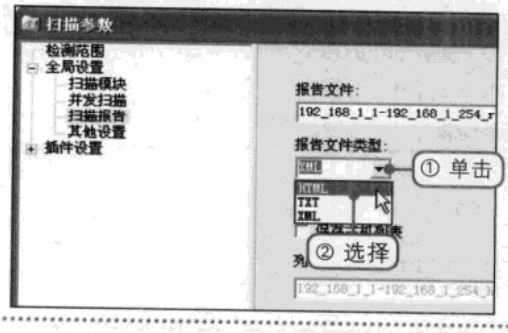
⑥ 设置并发扫描

选择“并发扫描”选项，设置并发扫描的主机数量和并发线程数，也可单独为每台主机的各个插件设置最大线程数。



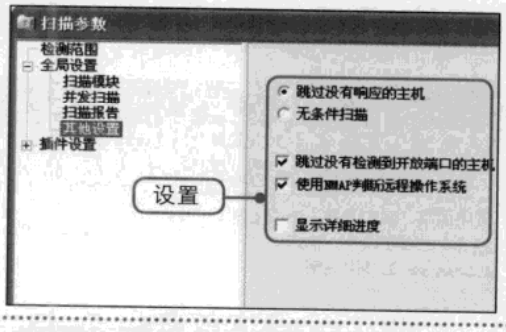
⑦ 设置扫描报告

选择“扫描报告”选项，①单击“报告文件类型”下拉列表框右侧的下三角按钮。②在弹出的下拉列表中选择HTML选项。



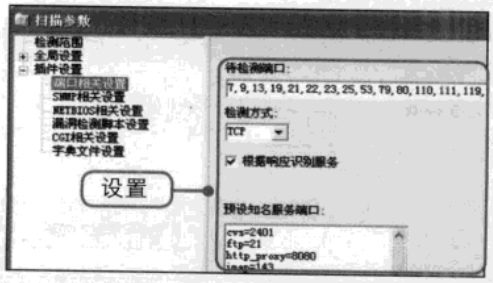
⑧ 其他设置

选择“其他设置”选项，在对话框右侧进行相关的设置。



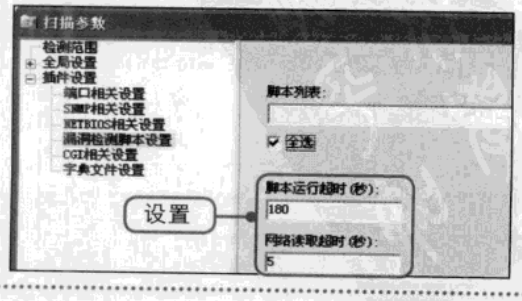
⑨ 端口相关设置

选择“插件设置>端口相关设置”选项，接着在右侧设置待检测端口、检测方式等选项。



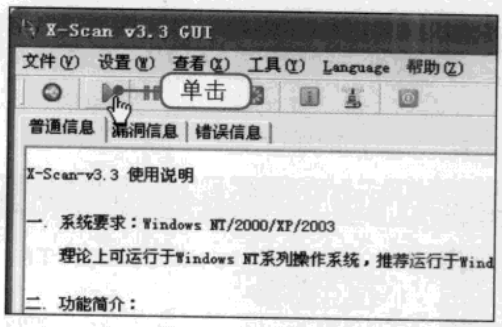
⑩ 漏洞检测脚本设置

选择“漏洞检测脚本设置”选项，接着在右侧设置脚本运行超时、网络读取超时等选项，然后单击“确定”按钮。



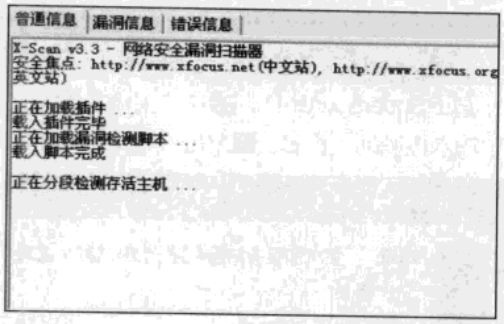
11 开始扫描

设置完毕后返回主界面窗口，在工具栏中单击“开始扫描”按钮开始扫描端口。



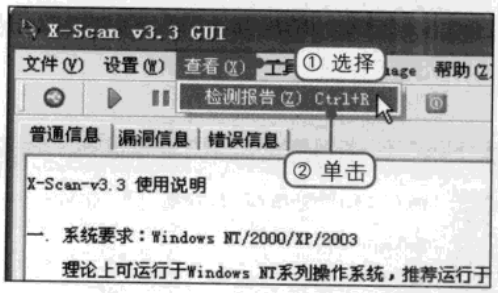
12 正在扫描

此时该软件正在扫描端口，可在窗口中查看扫描的详细信息，只需耐心等待即可。



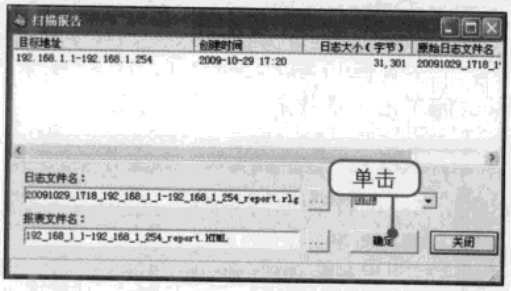
13 单击“检测报告”命令

返回主界面窗口，①在菜单栏中选择“查看”选项。②在弹出的菜单中单击“检测报告”命令，打开“扫描报告”窗口。



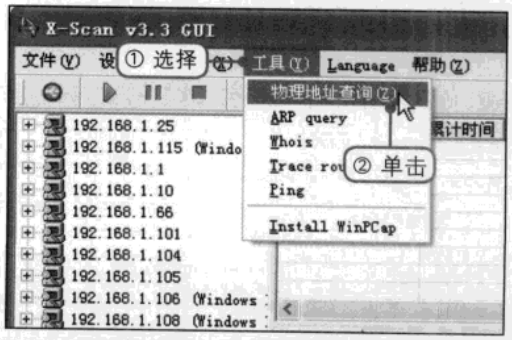
14 查看扫描报告

在“扫描报告”窗口中可以看到扫描报告，双击扫描报告即可看到网页形式的扫描报告窗口，查看完毕后单击“确定”按钮。



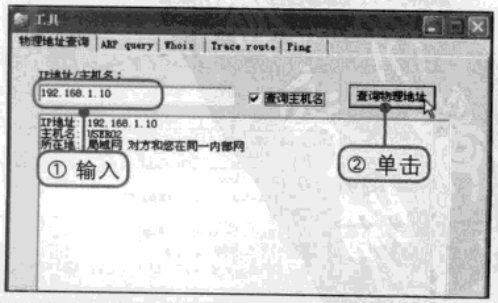
15 单击“物理地址查询”命令

返回主界面窗口，①选择菜单栏中的“工具”选项。②在弹出的菜单中单击“物理地址查询”命令。



16 查询物理地址

打开“工具”对话框，①在“IP地址/主机名”文本框中输入IP地址。②单击“查询物理地址”按钮即可在下方列表框中查看到对应的主机名和所在地。

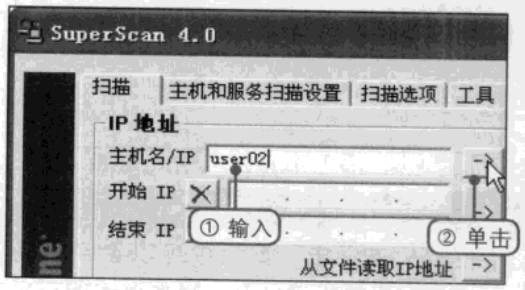


10.2.8 使用SuperScan进行端口扫描

SuperScan是一款功能十分强大的扫描软件，它不仅可以扫描端口，而且还可以自定义要检验的端口并保存为端口的列表文件。

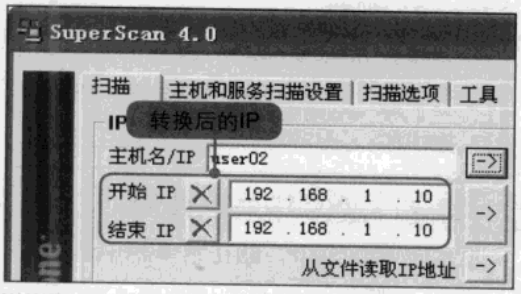
① 输入目标电脑的主机名

启动SuperScan软件，①在“主机名/IP”文本框中输入电脑的主机名。②单击“转换”按钮。



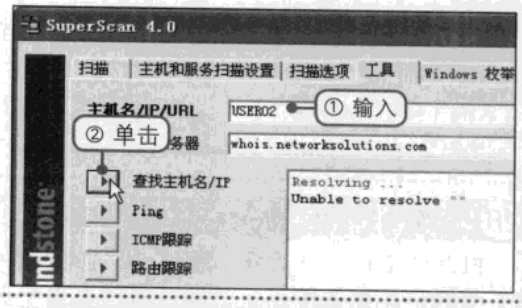
② 查看转换的IP地址

可在下方的“开始IP”和“结束IP”文本框中看见电脑的IP地址。



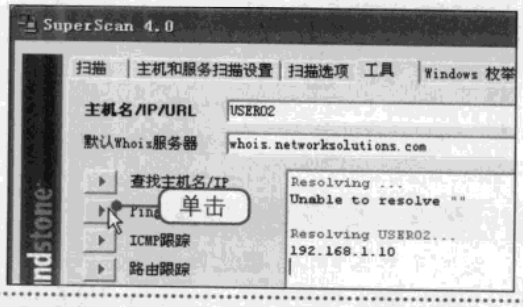
③ 单击“查找主机名/IP”按钮

①在“工具”选项卡中的“主机名/IP/URL”文本框中输入主机名、IP地址或者URL。②单击“查找主机名/IP”按钮。



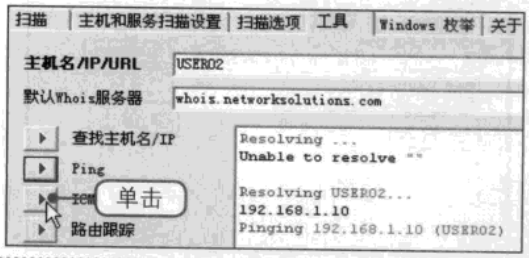
④ 单击Ping按钮

单击Ping按钮，如果能Ping通则说明这两台计算机是可以进行数据传输的。



⑤ ICMP跟踪

单击“ICMP跟踪”按钮即可对远程主机进行ICMP跟踪。

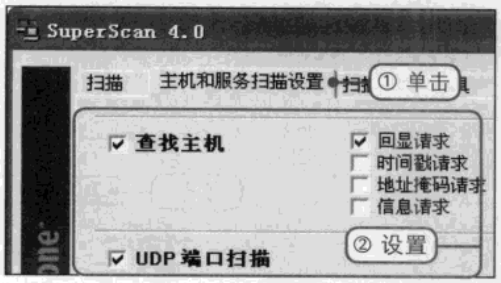


⑥ 路由跟踪

单击“路由跟踪”按钮即可对远程计算机进行路由跟踪。

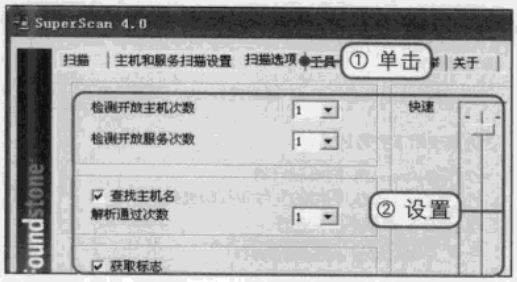
⑦ 设置主机和服务扫描

①单击“主机和服务扫描设置”标签切换至该选项卡。②然后对主机和服务扫描进行相关设置。



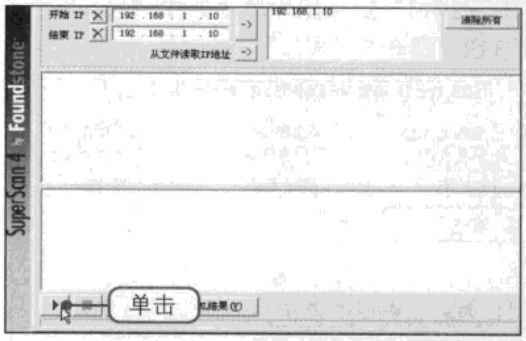
⑧ 设置扫描选项

①单击“扫描选项”标签切换至该选项卡。②设置一些扫描的基本信息。



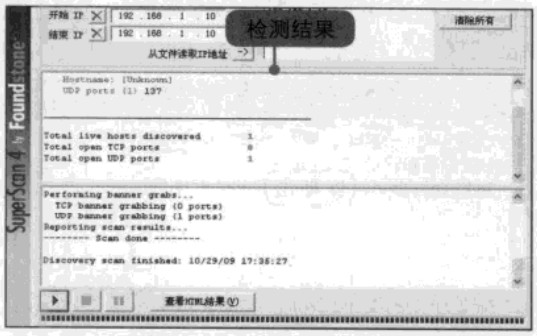
⑨ 开始检测

设置完毕后返回“扫描”选项卡，接着单击下方的“开始”按钮即可检测端口。



⑩ 检测完成

等待片刻之后检测完毕，此时可在窗口中看见检测的结果。

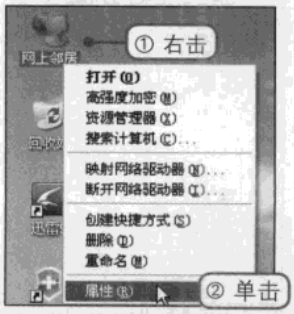


10.2.9 限制不必要的端口

安装操作系统后，有一些不安全并且没有什么用处的端口是默认开启的，如Telnet服务的23号端口、FTP服务的21号端口，等等，用户可使用TCP/IP筛选功能限制这些端口。

① 打开“网络连接”窗口

①右击“网上邻居”快捷图标。②在弹出的快捷菜单中单击“属性”命令。

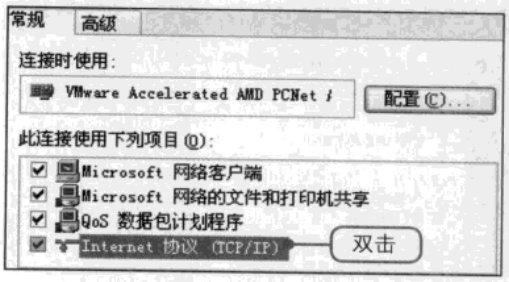


② 单击“属性”命令

打开“网络连接”窗口，①右击“本地连接”图标。②在弹出的快捷菜单中单击“属性”命令。

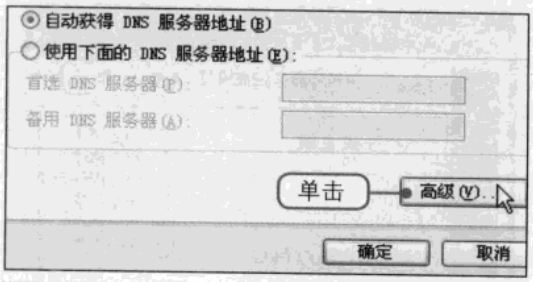
③ 双击“Internet协议”选项

打开“本地连接属性”对话框，双击“Internet协议（TCP/IP）”选项。



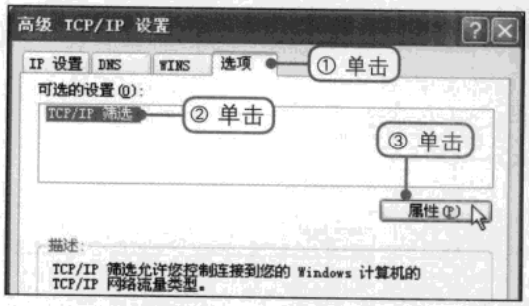
④ 单击“高级”按钮

打开“Internet协议属性”对话框，单击对话框下方的“高级”按钮。



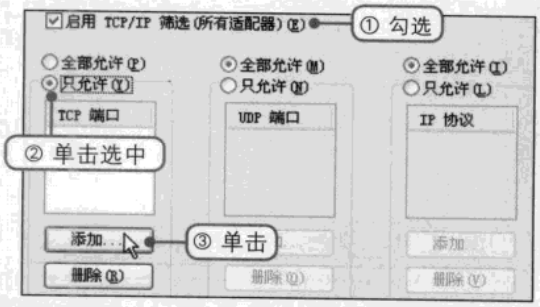
⑤ 打开“TCP/IP筛选”对话框

①在“高级TCP/IP设置”对话框中单击“选项”标签切换至该选项卡。②在“可选的设置”选项组中单击“TCP/IP筛选”选项。③单击“属性”按钮。



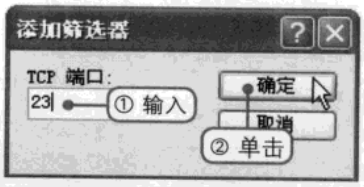
⑥ 设置TCP/IP筛选

打开“TCP/IP筛选”对话框，①勾选“启用TCP/IP筛选（所有适配器）”复选框，②在“TCP端口”选项组中单击选中“只允许”单选按钮。③单击“添加”按钮。



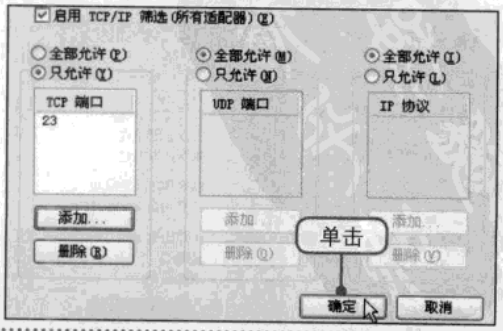
⑦ 输入允许的端口号

弹出“添加筛选器”对话框，①在“TCP端口”文本框中输入端口号，例如输入23，②单击“确定”按钮。



⑧ 保存退出

返回“TCP/IP筛选”对话框，用户可按照此方法设置其他端口，设置完毕后单击“确定”按钮保存退出即可。



10.3 黑客常用的命令

黑客攻击电脑也需要使用一些网络命令进行探测并获取信息，这些命令对黑客来说是最基本的，例如ping命令用于探测网络连接、net命令用于管理网络环境以及ftp命令用于进行数据传输，等等。

10.3.1 路由与网关

黑客入侵电脑离不开路由和网关，在介绍黑客常用的DOS命令之前先要理解路由和网关的基本概念。

1 路由

路由是指通过互相连接的网络把数据或者信息从初始地点传递到目的地，一般在路由的过程中，数据或者信息至少会经过一个中间节点。

2 路由器

路由器是实现路由功能的设备，是一种连接多个网络或网段的网络设备。它能将不同网络或网段之间的数据信息进行解读，以使它们能够相互“理解”对方的数据，从而构成一个更大的网络。路由器是互联网的主要设备节点。

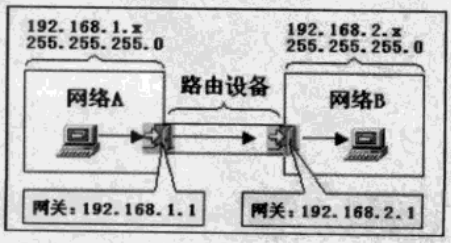
3 网关

网关又称为网间连接器、协议转换器。我们都知道若想从一个房间走到另一个房间，必然要经过一扇门。同样从一个网络向另一个网络发送信息，也必须经过一道“关口”，这道关口就是网关。网关就是一个网络连接到另一个网络的“关口”。

按照不同的分类标准，网关也有很多种。TCP/IP协议里的网关是最常用的，这里介绍的“网关”均指TCP/IP协议下的网关。

网关的实质是一个网络通向其他网络的IP地址。例如有网络A和网络B，网络A的IP地址范围为192.168.1.1~192. 168.1.254，子网掩码为255.255.255.0；网络B的IP地址范围为192.168.2.1~192.168.2.254，子网掩码为255.255.255.0。在没有路由器的情况下，两个网络之间是不能进行TCP/IP通信的，即使是两个网络连接在同一台交换机或集线器上，TCP/IP协议也会根据子网掩码判定两个网络中的主机处在不同的网络里。

要实现上述两个网络之间的通信，必须通过网关。如果网络A中的主机发现数据包的目的主机不在本地网络中，它就会把数据包转发给它自己的网关，再由网关转发给网络B的网关，网络B的网关再转发给网络B中的某个主机。如右图所示为网络A向网络B转发数据包的过程。

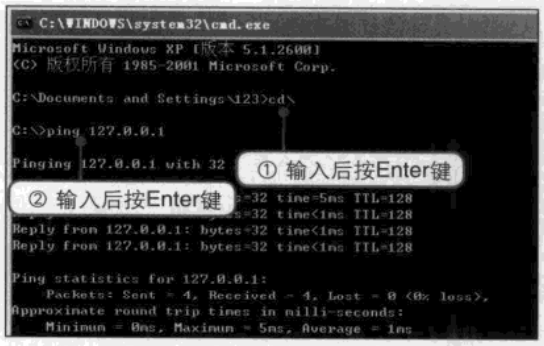


10.3.2 使用ping命令测试网络连接

Ping（Packet Internet Group，因特网探索器）命令，一般用于检测网络是否连通，是测试网络连接量的DOS命令。ping命令使用的前提是需要安装TCP/IP协议，其主要作用是通过发送数据包并接受应答信息来检测两台电脑之间的网络是否连通。当网络中出现故障时，用户可以使用这个命令来预测故障和确定故障的地点。

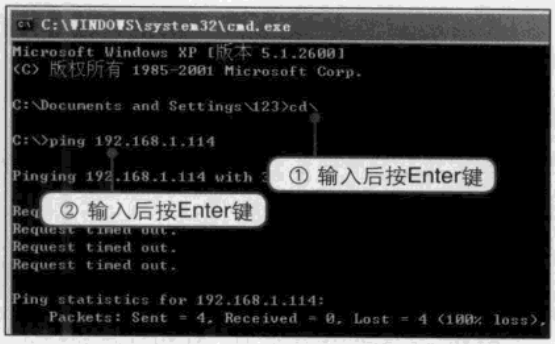
① 测试TCP/IP协议

打开“运行”对话框，输入cmd命令后按Enter键打开命令提示符，①输入“cd\”命令后按Enter键进入C盘根目录下，②输入“ping 127.0.0.1”后按Enter键，如果能ping通则说明已经安装了协议。



② 连通远程计算机

按照前面的方法打开命令提示符，①输入“cd\”命令后按Enter键进入C盘根目录下。②输入“ping+空格+IP地址”命令后按Enter键，若能ping通则说明连通成功，若没有连通则说明没有连通。



③ 获取NETBIOS主机名

按照前面的方法打开命令提示符，①输入“cd\”命令后按Enter键进入C盘根目录下。②输入“ping –a+IP地址”，例如输入“ping –a 192.168.1.115”后按Enter键便可在下面第一行中看见NETBIOS主机名。

④ 连续对IP地址执行ping命令

默认情况下ping命令只执行4次，而若要连续对IP地址执行ping命令则可在其命令后加上“空格–t”，如输入“ping 192.168.1.115 –t”后按Enter键，则将会连续执行ping命令，若要停止则可按Ctrl+C键将其强制终端。

127.0.0.1

127.0.0.1是回送地址，指本地机，一般在测试时使用，即用户可使用ping 127.0.0.1来测试本机TCP/IP是否正常。

ping命令的含义

用户在执行了ping命令以后会有返回的命令，当命令提示符中显示了“Reply from”字样时，则说明ping通了，如果显示“Request from out”字样时，则表示连接超时，无法ping通。

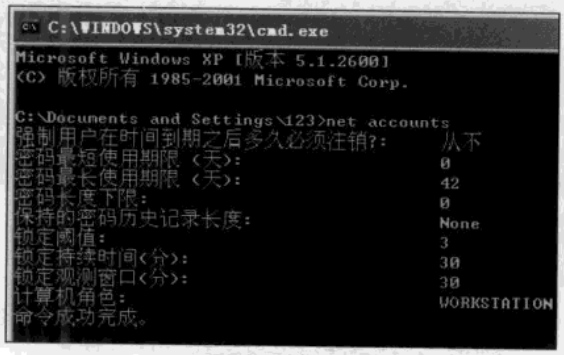
10.3.3 使用net命令管理网络环境

net命令是以命令行方式执行的工具，它的功能十分强大，包含了管理网络环境、服务、用户和登录等管理功能，用户使用该命令可以轻松地管理本地或者远程计算机的网络环境，以及各种服务程序的运行和配置，除此之外，使用该命令还可以进行用户管理和登录管理。

1 net account

net account该命令用于更新用户的账户数据库，并且为所有账户修改密码和登录需求。

打开命令提示符，接着输入 net account 命令后按Enter键。之后用户可在命令提示符中显示强制用户在时间到期之后多久必须注销、密码最短使用期限、密码最长使用期限、密码长度下限、保持的密码历史记录长度、锁定阈值、锁定持续时间、锁定观测窗口和计算机角色等详细信息。



该命令的格式为：*net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length] [/maxpwage:{days|unlimited}][/minpwage:days] [/uniquepw:number] [/sync] [/domain]*

net accounts命令的参数及其说明如表10-1所示。

表10-1 net account命令的参数与说明

参　数	说　明
不带参数	显示密码、登录限制和域信息的当前配置
/forcelogoff:{minutes | no}	设置当用户账户或有效登录时间到期时在结束用户与服务器的会话前要等待的分钟数
/minpwlen:length	设置用户账户密码的最少字符数
/maxpwage:{days | unlimited}	设置用户账户密码有效天数的最大值
/maxpwage:unlimited	设置账户密码永远有效
/minpwage:days	设置在用户可以更改新密码前的最小天数
/uniquepw:number	要求用户不对number次密码更改重复相同的密码
/sync	更新所有成员服务服务器的用户账户数据库
/domain	对当前域的主域控制器执行操作

2 net computer

net computer命令用于添加或者删除域数据库中的计算机，所有计算机的添加和删除都会转发到主域控制器。

该命令的格式为：*net computer \\computername {/add | /del}*

该命令的参数及说明如表10-2所示。

表10-2 net computer命令的参数与说明

参　数	说　明
\\computername：	指定要从域中添加或删除的计算机名
/add：	将特定的计算机添加到域中
/del：	从域中删除指定的计算机

3 net config

net config命令用于显示工作站或服务器服务的配置消息，或者显示并更改某项服务的设置。

打开命令提示符，接着输入 net config命令后按Enter键，用户可在命令提示符中看见如右图所示的界面，即显示了一个可配置服务的列表。

该命令的格式为：*net config [service [options]*
该命令的参数及说明如表10-3所示。

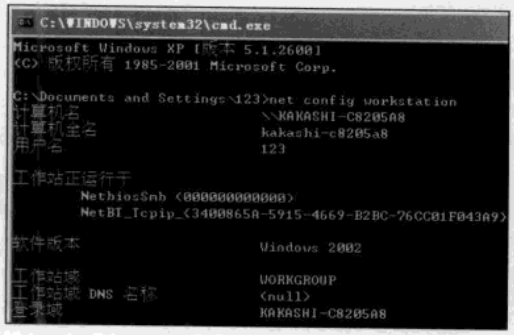
表10-3 net config命令的参数及说明

参　数	说　明
service：	通过net config命令进行配置的服务
options：	服务的特定选项

4 net config workstation

net config workstation命令用于显示更改可配置工作站服务参数，更改立即生效，并且永久保持。并非所有的工作站服务参数都能使用 net config workstation 命令进行更改，其他参数可以在配置注册表时修改。

打开命令提示符，接着输入net config workstation命令后按Enter键，用户可在命令提示符中看见如右图所示的界面，界面中显示了当前计算机名、计算机全名、用户名、软件版本、工作站域和工作站域DNS名称等详细信息。



该命令的格式为：*net config workstation [/charcount:bytes] [/chartime:msec] [/charwait:sec]*
该命令的参数及说明如表10-4所示。

表10-4 net config workstation命令的参数及说明

参　数	说　明
/charcount:bytes	指定在将数据发送到通信设备之前Windows 收集的数据量。如果还设置了/chartime:msec，Windows 将执行第一个满足的选项。范围是0～-65535字节，默认值是16字节
/chartime:msec	设置 Windows在将数据发送到通信设备前收集数据的毫秒数。如果还设置了/charcount:bytes，Windows将执行第一个满足的选项。范围是0～65535000毫秒，默认是250毫秒
/charwait:sec	将Windows等待通信设备的秒数设置为可用。范围是0～65535s，默认值是3600s。例如要设置在将数据发送到最大1000毫秒的通信设备之前Windows等待。则可使用net config workstation /chartime:1000

5 net contiune

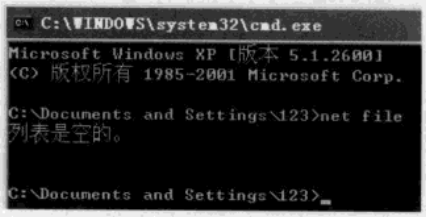
该命令能够重新激活挂起的服务。
该命令的格式为：*net continue service*

能够继续运行的服务，包括file server for macintosh（该服务仅限于 Windows NT Server），ftp publishing service, lpdsvc, net logon, network dde, network dde dsdm, nt lm security support provider, remoteboot（该服务仅限于 Windows NT Server），remote access server, schedule, server, simple tcp/ip services 及 workstation。

6 net file

net file命令用于显示某服务器上所有打开的共享文件夹及锁定文件数。该命令也可以关闭个别文件并取消文件锁定。

打开命令提示符，接着输入 net file命令后按Enter键，若服务器上有打开文件的列表，用户可在命令提示符中看见其详细信息。



该命令的格式为：*net file [id [/close]]*

该命令的参数及说明如表10-5所示。

表10-5 net file命令及参数说明

参数	说明
id	文件标识号
/close	关闭打开的文件并释放锁定记录。请从共享文件的服务器中键入该命令

7 net group

net group命令用于在 Windows NT Server 域中添加、显示或更改全局组，仅在Windows NT Server域中可用。

该命令的格式为：*net group [groupname [/comment:"text "]] [/domain]*
net group groupname {/add [/comment:"text "] | /delete} [/domain]
net group groupname username [...] {/add | /delete} [/domain]

该命令的参数及说明如表10-6所示。

表10-6 net group命令及参数说明

参数	说明
groupname	要添加、扩展或删除的组。仅提供某个组名便可查看组中的用户列表
/comment:"text "	为新建组或现有组添加注释。注释最多可以是48个字符，并用引号将注释文字引住
/domain	在当前域的主域控制器中执行该操作，否则在本地计算机上执行操作。该参数仅用于作为Windows NT Server域成员的 Windows NT Workstation计算机
username[...]	列表显示要添加到组或从组中删除的一个或多个用户
/add	添加组或在组中添加用户名。必须使用该命令为添加到组中的用户建立账号
/delete	删除组或从组中删除用户名

8 net help

net help命令用于提供网络命令列表及帮助主题，或者提供指定命令或主题的帮助。

打开命令提示符，接着输入 net help命令后按Enter键，用户可在命令提示符中看见能够获得帮助的命令列表和帮助主题。

该命令的格式为：*net help [command] net command {/help | /?}*

该命令的参数及说明如表10-7所示。

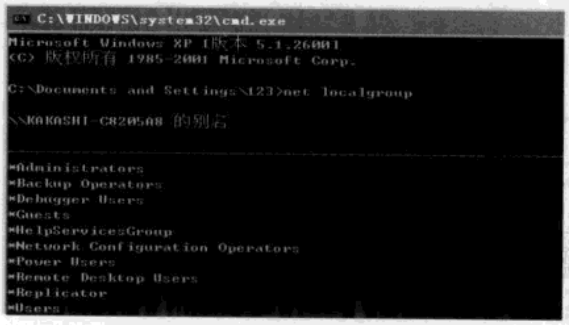
表10-7　net help命令参数及说明

参　数	说　明
/help	提供显示帮助文本方式选择
/?	显示命令的正确语法

9 net localgroup

net localgroup命令用于显示、删除或者更改本地组。

打开命令提示符，接着输入 net localgroup命令后按Enter键。用户可在命令提示符中看见服务器的名称以及计算机的本地组名称。



该命令的格式为：*net localgroup [groupname [/comment:"text "]] [/domain]*

net localgroup groupname {/add [/comment:"text "] | /delete} [/domain]

net localgroup groupname name [...] {/add | /delete} [/domain]

该命令的参数及说明如表10-8所示。

表10-8 net localgroup命令参数及说明

参　数	说　明
groupname	要添加、扩充或删除的本地组名称,只提供 groupname即可查看用户列表或本地组中的全局组
/comment:"text "	为新建或现有组添加注释。注释文字的最大长度是48个字符，并用引号引住
/domain	在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作。该参数仅应用于Windows NT Server域中的Windows NT Workstation计算机
name[...]	列出要添加到本地组或从本地组中删除的一个或多个用户名或组名，多个用户名或组名之间以空格分隔。可以是本地用户、其他域用户或全局组，但不能是其他本地组。如果是其他域的用户，要在用户名前加域名
/add	将全局组名或用户名添加到本地组中。在使用该命令将用户或全局组添加到本地组之前，必须为其建立账号
/delete	从本地组中删除组名或用户名

10 net name

net name命令用于添加或者删除消息名（有时称别名），或者显示计算机接收消息的列表。用户若要使用该命令，则计算机中必须运行信使服务。

打开命令提示符，接着输入 net name命令后按Enter键。若启动了Message服务，则会在命令提示符中看见其服务的详细信息。

该命令的格式为：*net name [name [/add | /delete]]*

该命令的参数及说明如表10-9所示。

表10-9 net name命令参数及说明

参　数	说　明
name	指定接收消息的名称。名称最多为 15 个字符
/add	将名称添加到计算机中。/add是可选项，键入net name name与键入net name name /add相同
/delete	从计算机中删除名称

11 net print

net print命令用于显示或控制打印作业及打印队列。

该命令的格式为：*net print \computername*

net print \sharename

net print [\computername] job# [/hold | /release | /delete]

该命令的参数及说明如表10-10所示。

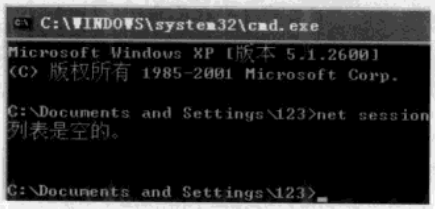
表10-10 net print命令参数及说明

参　数	说　明
computername	共享打印机队列的计算机名
sharename	打印队列名称。当包含computername与sharename时，使用反斜杠将它们分开
job#	在打印机队列中分配给打印作业的标识号。有一个或多个打印机队列的计算机为每个打印作业分配唯一标识号。如果某个作业号用于共享打印机队列中，则不能指定给其他作业，也不能分配给其他打印机队列中的作业
/hold	使用job# 时，在打印机队列中使打印作业等待。打印作业停留在打印机队列中，并且其他打印作业只能等到释放该作业之后才能进入
/release	释放保留的打印作业
/delete	从打印机队列中删除打印作业

12 net session

net session命令用于列出或断开本地计算机和与之连接的客户端的会话。

打开命令提示符，接着输入net session命令后按Enter键。在命令提示符中可以显示所有与本地计算机的会话信息。



该命令的格式为：*net session [\computername] [/delete]*

该命令的参数及说明如表10-11所示。

表10-11 net session命令参数及说明

参　数	说　明
\computername	标识要列出或断开会话的计算机
/delete	结束与 \computername 计算机会话并关闭本次会话期间计算机的所有打开文件。如果省略\computername 参数，将取消与本地计算机的所有会话

13 net send

net send命令用于向网络的其他用户、计算机发送消息。要接收消息必须运行信使服务。

该命令的格式为：*net send {name | * | /domain[:name] | /users} message*

该命令的参数及说明如表10-12所示。

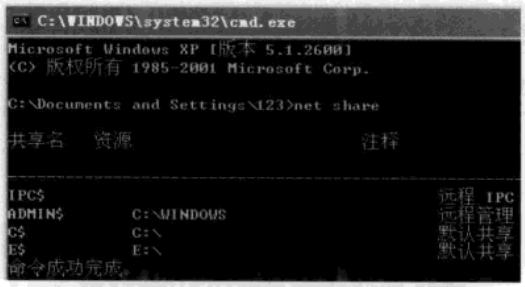
表10-12 net send命令参数及说明

参　数	说　明
name	要接收发送消息的用户名、计算机名或通信名
*	将消息发送到组中所有名称
/domain[:name]	将消息发送到计算机域中的所有名称
/users	将消息发送到与服务器连接的所有用户
message	作为消息发送的文本

14 net share

net share命令用于创建、删除或者显示共享资源。

打开命令提示符，接着输入 net share命令后按Enter键。用户将在命令提示符中看见本地计算机上所有共享资源的信息。



该命令的格式为：*net share sharename*

net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]

net share sharename [/users:number | unlimited] [/remark:"text"]

net share {sharename | drive:path} /delete

该命令的参数及说明如表10-13所示。

表10-13 net share命令参数及说明

参　数	说　明
sharename	是共享资源的网络名称。键入带 sharename 的 net share 命令，只显示该共享信息
drive:path	指定共享目录的绝对路径
/users:number	设置可同时访问共享资源的最大用户数
/unlimited	不限制同时访问共享资源的用户数
/remark:"text "	添加关于资源的注释，注释文字用引号引住
/delete	停止共享资源

15 net time

net time命令用于使计算机的时间与另一台计算机或域的时间同步。不带/set参数使用时，将显示另外一台计算机或域的时间。

该命令的格式为：*net time [\computername | /domain[:name]] [/set]*

该命令的参数及说明如表10-14所示。

表10-14 net time命令参数及说明

参　数	说　明
\computername	要检查或同步的服务器名
/domain[:name]	指定要与其时间同步的域
/set	使本计算机时钟与指定计算机或域的时钟同步

10.3.4 使用telnet命令进行远程登录

telnet是一个非常实用并且功能十分强大的命令，可以使用该命令进行远程登录。该命令允许用户使用telnet协议在远程计算机之间进行通信，用户可以通过网络在远程计算机上登录，就像登录到本地计算机上执行命令一样。

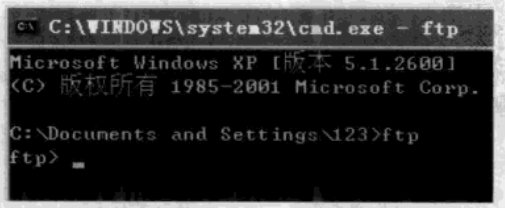
telnet命令的格式为：telnet+空格+IP地址/主机名名称。例如使用“telnet 192.168.1.115”执行成功，则将从IP地址为192.168.1.115的远程计算机上得到login:提示符。

使用telnet命令登录的过程如下：输入“$telnet主机名/IP”启动telnet会话。一旦telnet成功地连接到远程计算机上，就显示登录信息并提示用户输入用户名和口令。若用户输入正确，就能成功地登录并在远程计算机上工作。

10.3.5 使用ftp命令进行数据传输

ftp命令是互联网用户使用最频繁的命令之一，不论是在DOS还是在UNIX操作系统下使用ftp都会遇到大量的ftp内部命令。用户使用ftp命令可以将文件传送到正在运行ftp服务的计算机中，或者从正在运行ftp服务的计算机上传送文件，它们可以交互使用。

按照前面的方法打开命令提示符，接着输入ftp命令后按Enter键。此时进入ftp子环境的界面，用户就可连接正在运行ftp服务的远程计算机进行相关的操作了。



FTP命令的格式为：*FTP –v –d –I –n –g [主机名]*

该命令的参数及说明如表10-15所示。

表10-15 ftp命令参数及说明

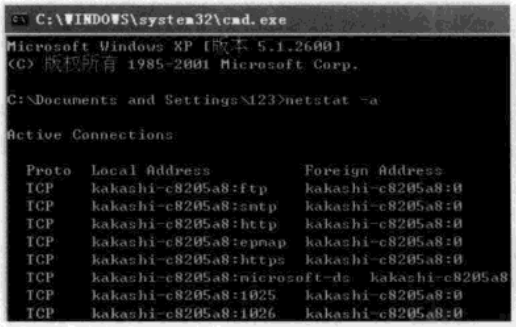
参　数	说　明
-v	显示远程服务器的所有响应信息
-d	使用调试方式，显示在客户端和服务器之间传递的ftp命令
-i	传送多个文件时关闭交换提示
-n	限制ftp的自动登录，即不使用
-g	取消全局文件名

10.3.6 使用netstat命令查看网络连接的相关信息

netstat命令显示网络连接、路由表和网络接口信息，可以使用户得知目前都有哪些网络连接正在运行。该命令的格式为：*netstat[-a][-b][-e][-n][-o][-p proto][-r][-s][-v][interval]*

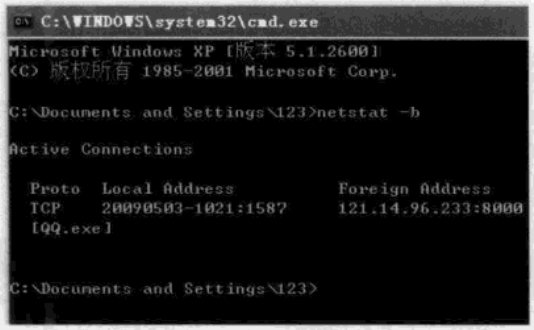
① 使用 netstat -a命令

使用netstat –a命令能显示所有连接和监听端口。



② 使用 netstat -b命令

使用netstat –b命令能显示包含创建每个连接或者监听端口的可执行文件。

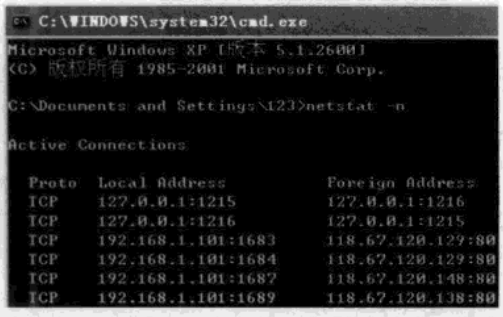


③ 使用 netstat -e命令

使用netstat –e命令能显示以太网数据统计，该参数可以与–s结合使用。

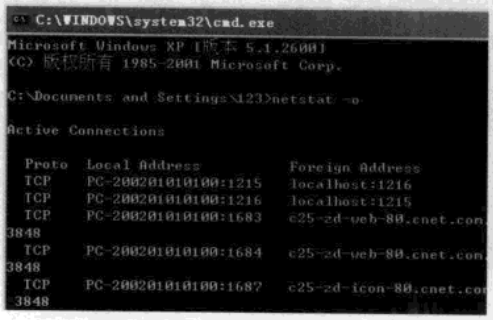
④ 使用 netstat -n命令

使用netstat –n命令能以网络IP地址代替名称，显示出网络连接情形。



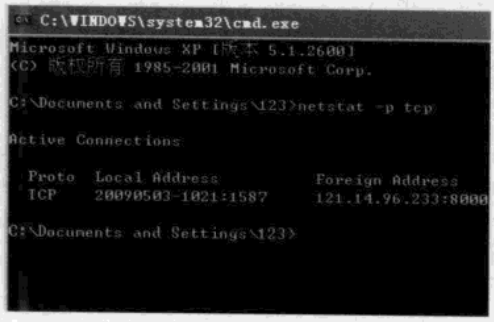
⑤ 使用 netstat -o命令

使用netstat –o命令能显示与每个连接相关的所属进程ID。



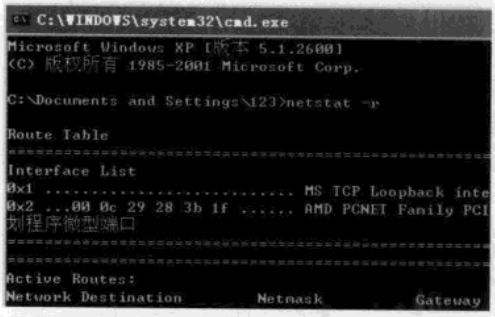
⑥ 使用 netstat -p proto命令

使用该命令能显示指定协议的连接，proto是指协议（Protocol），它可以是TCP或UDP。



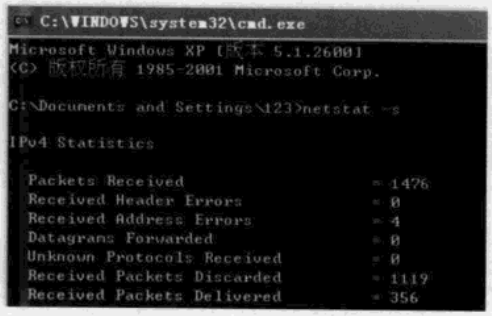
⑦ 使用 netstat -r命令

使用netstat –r命令能在命令提示符中打开路由选择表。



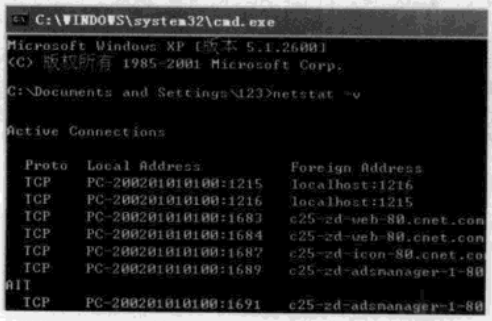
⑧ 使用 netstat -s命令

使用netstat –s命令能在机器默认情况下显示每个协议的配置统计，包括TCP、IP、UDP或ICMP等协议。



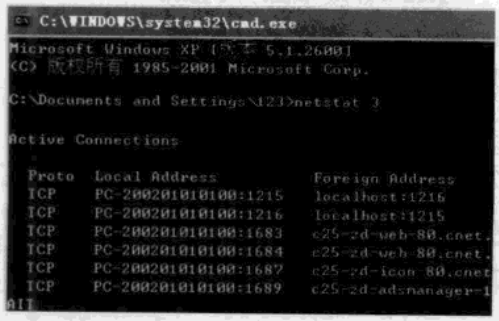
⑨ 使用netstat -v命令

netstat –v命令与–b参数一起使用时将包含为所有可执行组件创建连接或监听端口的组件。



⑩ 使用netstat interval命令

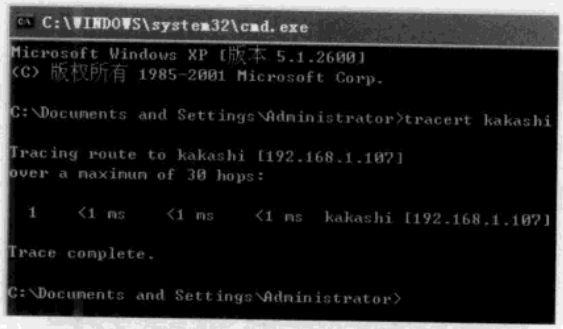
每隔interval秒将重复显示所选协议的配置情况，直到按Ctrl+C键中断为止，例如输入“netstat 3”则表示每3秒显示重复的协议。



10.3.7 使用tracert命令查看IP数据报的传输路径

tracert是路由跟踪实用程序，该命令用于确定IP数据报访问目标所采取的路径，它通过使用IP生存时间字段（TTL）和ICMP报文错误消息来确认从一个主机到网络上其他主机的路由。

打开命令提示符，输入tracer+空格+主机名后按Enter键，此时可在命令提示符中看见该主机名对应的IP地址。例如输入tracert kakashi后按Enter键，接着就可看见对应的IP地址（192.168.1.107）和其他信息。



该命令的格式为：*tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name*

参数及说明如表10-16所示。

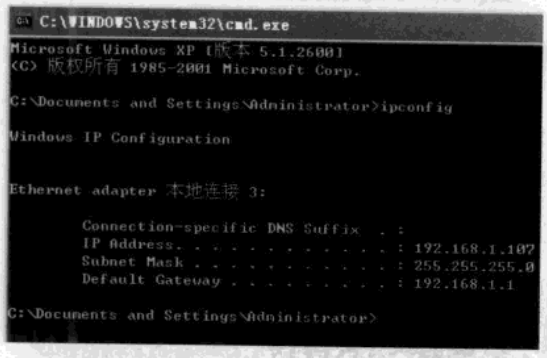
表10-16 tracert命令参数及说明

参　数	说　明
-d	指定不将IP地址解析到主机名称
-h maximum_hops	指定跃点数以跟踪到称为target_name的主机的路由
-j host-list	指定tracert实用程序数据报所采用路径中的路由器接口列表
-w timeout	等待timeout为每次回复所指定的毫秒数
target_name	目标主机的名称或IP地址

10.3.8 使用ipconfig命令检测配置的TCP/IP

ipconfig命令用于显示所有当前的TCP/IP网络配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。使用不带参数的ipconfig命令可以显示所有适配器的IP地址、子网掩码和默认网关。

打开命令提示符，输入ipconfig命令后按Enter键即可在命令提示符中看见当前电脑的IP地址、子网掩码和默认网关，如右图所示，当前电脑的IP地址为192.168.1.107，子网掩码为255.255.255.0.默认网关为192.168.1.1。



该命令的格式为：*ipconfig[/all][/renew[adapter][/release[adapter]*

该命令的参数及说明如表10-17所示。

表10-17 ipconfig命令及参数说明

参　数	说　明
/all	显示所有适配器的完全TCP/IP配置信息
/renew[adapter]	更新DHCP配置参数。该参数只在运行DHCP客户端服务的系统上可用，要指定适配器名称，则需输入使用不带参数的ipconfig命令显示适配器的名称
/release[adapter]	发布当前的DHCP配置，该选项禁用本地系统上的TCP/IP，并只在DHCP客户端上可用。要指定适配器名称，则需直接输入使用不带参数的ipconfig命令显示的适配器名称

DHCP

DHCP是Dynamic Host Configuration Protocol的缩写，中文译为动态主机配置协议。该协议允许服务器向客户端动态分配IP地址和配置信息。通常DHCP服务器至少给客户端提供IP地址、子网掩码和默认网关等基本信息，它还可以提供域名服务（DNS）服务器地址和Windows Internet命名服务（WINS）服务器地址。系统管理员配置DHCP服务器分配给客户端的选项。

10.4 黑客常使用的入侵手段

了解了黑客常用的命令之后，需要了解黑客常用的入侵手段，如抓住系统漏洞、使用电子邮件进行攻击、使用木马程序和破解密码等手段，用户了解了这些常用的方法之后便可更好地防范黑客入侵。

1 抓住系统漏洞

黑客最常用的就是抓住系统漏洞进行攻击，当目标电脑的系统存在漏洞时，黑客只需要知道该电脑的IP地址以及操作系统的版本便可进行攻击。许多系统都有大大小小的漏洞，其中最常见的是操作系统或者应用软件的缺陷，有些漏洞在补丁程序没有开发出来之前几乎是没有办法防范的，因此用户需要及时下载并安装升级补丁或者安装最新版本的应用软件。还有一些系统漏洞是由于开发程序人员自身的大意造成的，相关的程序员通常喜欢在某一模块中加入调试代码以方便调试，当整个软件开发完成时再将这些代码删除，但是由于疏忽很有可能留下某些调试代码，这就给了黑客入侵电脑的机会。

2 使用电子邮件进行攻击

电子邮件（E-Mail）是互联网上应用非常广泛的一种通信服务，黑客通常使用一些炸弹邮件或者CGI程序向目标邮箱发送大量的垃圾邮件，“炸”掉邮箱。当多台电脑同时发送垃圾邮件时很可能造成邮件系统反应缓慢，甚至瘫痪。除此之外，黑客还通常采用在邮件附件中添加木马或者病毒的方式攻击用户计算机，一旦用户打开该邮件携带的附件，木马和病毒就被成功的植入电脑中，黑客入侵成功。因此用户在打开电子邮件和附件时要格外慎重，陌生人的邮件千万不要轻易打开，并且在电脑中同时开启防火墙和杀毒软件，以确保安全。

3 使用木马程序

木马是一种远程控制软件，黑客利用木马进行攻击一般都需要在目标电脑的系统中隐藏一个随着Windows启动而自动启动的程序，然后采用服务器/客户机的运行方式达到控制目标电脑的目的。当用户电脑被植入木马之后，黑客几乎可以得到目标电脑的所有信息并且可对该电脑进行任何操作，如窃取账户和密码、更改文件操作、捕捉屏幕和修改注册表等。由于木马程序十分强大并且操作简单，因此成为大多数黑客的最爱。

4 破解密码

互联网上为了保护个人的隐私，用户所使用的账号都对应有一个密码，例如登录MSN需要密码、登录QQ需要密码、登录电子邮箱需要密码、登录计算机需要密码，等等，由于密码和账户配对，因此不管是谁，只要输入正确的账户和密码，均可进行后面的操作，因此黑客会尝试着破解用户的相关密码。向目标电脑中植入密码可以获取账号和密码，但是如果用户电脑中安装了杀毒软件，这种成功率就很小，除此之外，黑客也可以使用密码字典来破解相关的密码，即“暴力破解”，其工作原理是提取密码字典中的密码项，然后再一个个的尝试，只要密码字典足够大，其中的密码项足够多时便可破解该密码。

5 数据驱动攻击

有些特殊程序表面看上去没有什么害处，但是若把它发送或者复制到网络主机上并被执行发送攻击时，就会产生数据驱动攻击。例如一种数据驱动的攻击可以导致一台主机修改与网络安全有关的文件，这就使得黑客下一次入侵该系统更加容易。

6 跳跃式攻击

由于现在因特网上的站点都是用UNIX操作系统，因此黑客们会设法先登录到一台UNIX主机，通过系统漏洞取得系统特权，然后再以此为据点访问其余的主机，这种做法称为跳跃。黑客在达到目的主机之前往往会跳跃很多次。例如一名黑客在入侵美国联邦调查局的网络之前，可能会先登录到亚洲的一台主机上，接着再从亚洲的主机上登录到墨西哥的一台主机上，然后通过同样的方法再登录到欧洲，最后从瑞典的一台主机向目标网络发动攻击，这样的攻击即使发现了黑客是从何处向自己发起攻击，管理员也很难找到真实的位置，再加上每当黑客取得某台主机的系统特权之后，可以在退出时删除系统日以断绝联系。因此跳跃式攻击成为了黑客和安全专家们的共同关注点。

10.5 禁止IE浏览器Web脚本以防黑客攻击

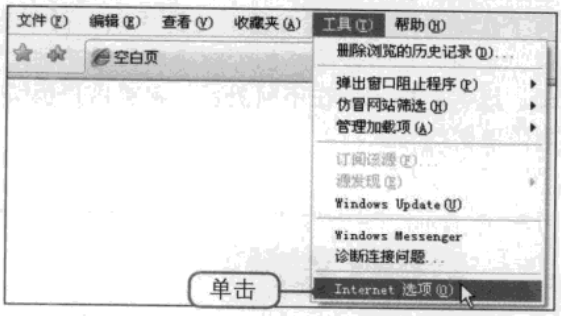
在使用聊天工具聊天时，有时会遇到屏幕上不断弹出警告或者错误对话框，无论怎么关也没有办法把它们全部关闭，其实这就是其他人给你发送的一段死循环HTML语句。这种工具的前提是聊天室允许使用HTML语言的功能，用户可以禁用IE浏览器的Web脚本以确保安全。

① 双击IE浏览器快捷图标

在桌面上双击Internet Explorer快捷图标，打开IE浏览器窗口。

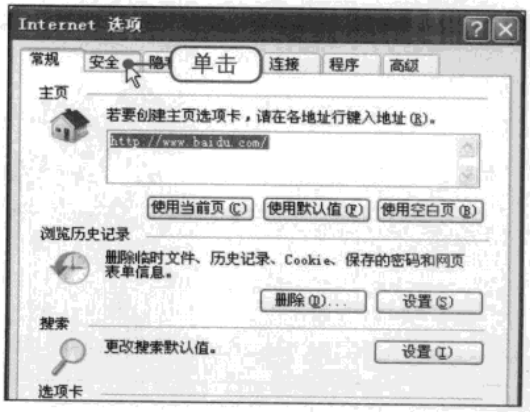
② 打开“Internet选项”对话框

单击菜单栏中的“工具>Internet选项”命令，打开“Internet选项”对话框。



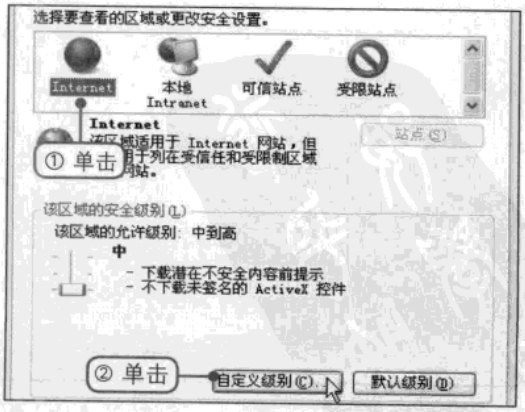
③ 切换至“安全”选项卡下

在对话框中单击“安全”标签切换至该选项卡。



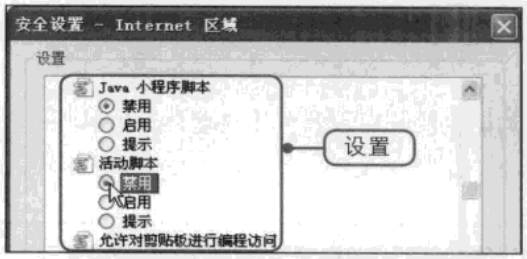
④ 单击“自定义级别”按钮

①单击Internet图标。②单击“自定义级别”按钮。



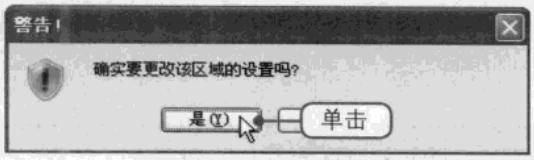
⑤ 禁止脚本运行

打开“安全设置-Internet区域”对话框，分别在“Java小程序脚本”和“活动脚本”选项组中单击选中“禁用”单选按钮。



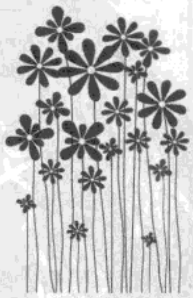
⑥ 使用 netstat -s命令

单击“确定”按钮后弹出“警告！”提示框，提示用户是否确认要更改该区域的设置，确认后单击“是”按钮即可。



本章介绍了黑客的基本知识，希望用户能够更好地保障自己电脑的安全，所谓知己知彼，百战百胜。若某些用户想要进一步了解黑客，仅本书的内容是不够的，本书介绍黑客的目的是为了让用户了解黑客入侵电脑的手段，而不是让用户成为一名黑客。黑客方面的内容十分广泛，本书只是十分粗略的介绍了黑客的基础知识和最常用的入侵手段，随着系统补丁的不断出现，黑客的技术也在不断更新，希望用户能够以电脑安全为出发点，通过设置电脑最大限度地保障电脑的安全。

读书笔记



Chapter 11

嗅探攻防

重点知识

1. 认识嗅探器
2. 嗅探攻击
3. 防范Sniffer

所谓嗅探（Sniff），是指用于监控网络上流经数据包的一种手段，而对于嗅探器Sniffer，被不同的人所使用，其产生的效果也不一样。当被网络管理员使用时就可监视网络中的数据包以保障网络安全，而当被黑客使用时，就会被窃听并截获有用的数据包，对网络安全造成一定的影响。本章将介绍嗅探器的基本知识，常见的嗅探器和用法，以及防范嗅探的常用方法。

视频文件

参见随书光盘：视频教程\Chapter 11

Chapter 11 嗅探攻防

11.2.1 嗅探MSN聊天记录
11.2.2 使用Sniffer Portable捕获报文
11.2.3 使用Sniffer Portable编辑并发送报文
11.2.4 使用艾菲网页侦探捕获网页内容

11.1 认识嗅探器

嗅探器是一种监视网络数据运行的软件设备，是协议分析器中的一种，它既能用于合法的网络管理，也能用于窃取相关的网络信息。非法嗅探器严重威胁了网络的安全性，这是由于它实质上不能进行探测行为且容易随处插入，因此常常被黑客作为攻击的武器。

嗅探器可以说是一把双刃剑，在网络管理员的手中，能够帮助用户监控网络流量，更好地管理网络，但是在黑客的手中，它却成为捕获计算机用户因为疏忽而带来的漏洞的工具。

网络嗅探器是网络管理员最常用的工具之一，简单地说，网络嗅探器就是使用户能够“嗅探”到本地网络的数据，并检查进入电脑的信息包；另外，当用户处理自身的网络问题时，一个信息包嗅探器可以向用户展示出正在网络上进行的一切活动，于是借助一定的知识，用户就可以确定问题的根源所在。信息嗅探器不会告诉用户“问题究竟是什么”,只会告诉用户“究竟发生了什么”。

在以前，当网络集线器还被用来进行所有办公网络设备连接的时候，用嗅探器来“嗅探”网络是一个十分简单的工作，而现在，交换机的工作方式使得嗅探器的使用变得十分复杂，即嗅探器无法抓取所有的信息包。当有大量信息包嗅探器的时候，用户必须认真地选择并决定最符合自己需求的信息包。每一个嗅探器都有优势和劣势，如何使用取决于用户自己的使用习惯和工作者对此嗅探器的要求。

协议分析器

协议分析器是指网络协议分析所使用的软件和设备，网络协议分析是指通过程序分析网络数据包的协议头和尾，从而了解信息和相关的数据包在产生和传输过程中的行为。网络运作和维护都可以采用协议分析器，如监视网络流量、分析数据包、监视网络资源利用、执行网络安全操作规则，鉴定分析网络数据以及诊断并修复网络问题等。

11.2 嗅探攻击

黑客们往往利用嗅探器获取信息包，并对信息包进行分析以获取网络中传输的一些重要信息，然后通过网络扫描和侦听获取想要的密码等信息。这里将介绍嗅探MSN聊天记录、通过网页登录账号嗅探密码、使用Sniffer Portable捕获数据以及使用“艾菲尔网页侦探”捕获网页内容。

>> 11.2.1 嗅探MSN聊天记录

MSN（Microsoft Service Network，微软网络服务）是一个出自微软的即时通信工具，与QQ

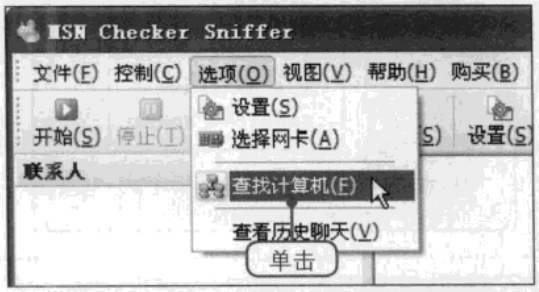
是同一个类别的工具。由于MSN在网络中被广泛地使用，因此一些黑客可以通过MSN checker sniffer来嗅探其聊天记录。

① 启动MSN checker Sniffer

用户下载并安装好MSN Checker Sniffer软件后会在桌面上出现对应的快捷图标，双击该图标，启动该应用程序，打开MSN Checker Sniffer主界面。

② 单击“查找计算机”命令

在菜单栏中单击“选项>查找计算机”命令，打开“查找计算机”对话框。

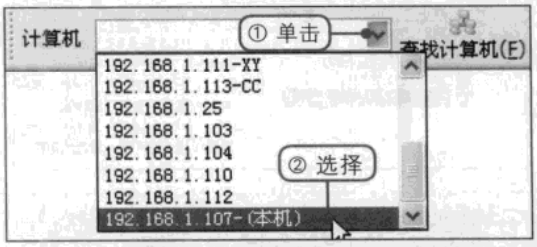


③ 通过IP地址扫描计算机

①在“开始IP地址”和“结束IP地址”文本框中输入IP地址。②单击“扫描”按钮，片刻之后结果显示在列表框中。

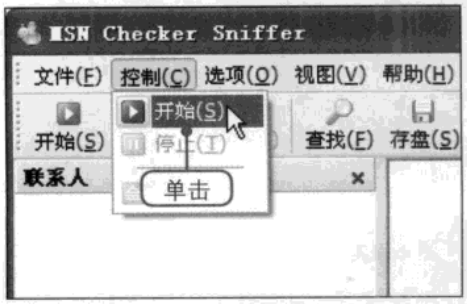
④ 选择嗅探的计算机

单击“确定”按钮返回主界面，①在工具栏中单击“计算机”下拉列表框右侧的下三角按钮。②在弹出的下拉列表中选择嗅探的计算机。



⑤ 开启嗅探功能

在主界面窗口中单击菜单栏中的“控制>开始”命令开启嗅探功能。

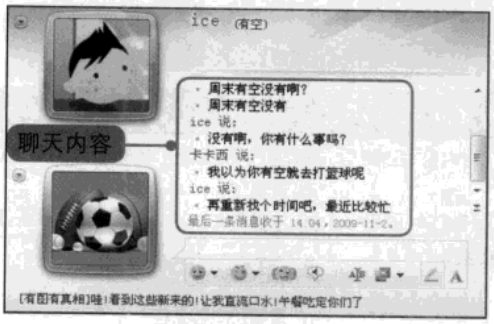


⑥ 登录MSN并选择聊天对象

由于前面操作步骤中选择的是本地计算机，则启动并登录MSN，双击“常用联系人”选项组下的好友头像，打开聊天窗口。

⑦ 开始聊天

在聊天窗口中尝试着与好友聊一段时间，用户可在窗口中看见与好友聊天的具体内容。

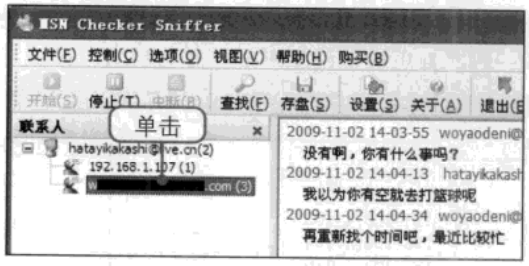


⑧ 嗅探成功

返回MSN Checker Sniffer主界面窗口，此时可以看见MSN聊天窗口中的聊天内容全部被记录到该窗口中，即嗅探成功。

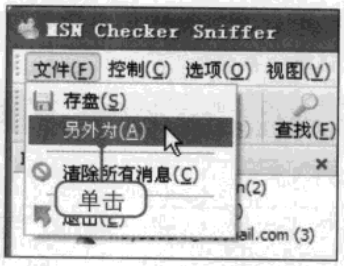
⑨ 选中联系人

若用户需要保存聊天的内容，则需首先在主界面窗口左侧单击联系人。



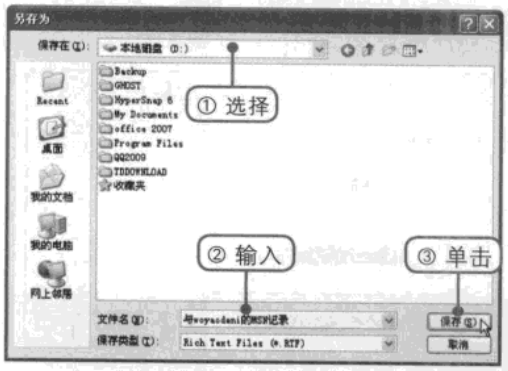
⑩ 单击“另存为”命令

单击菜单栏中的“文件>另存为”命令，打开“另存为”对话框。



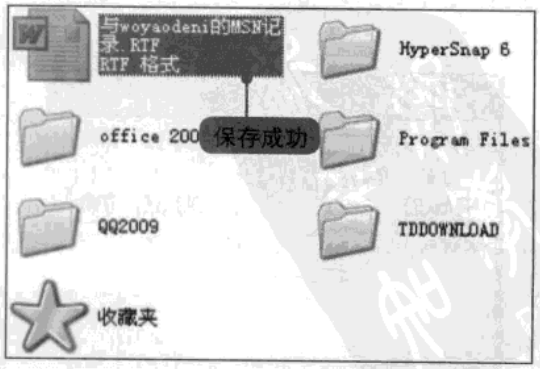
⑪ 设置保存路径和文件名

①在“保存在”下拉列表中选择保存的位置。②在“文件名”文本框中输入文件名。③单击“保存”按钮。



⑫ 保存成功

打开保存位置所在的窗口，此时可在窗口中看见保存的内容记录在Word文档中，双击该文件即可查看对应的内容。



11.2.2 使用Sniffer Portable捕获报文

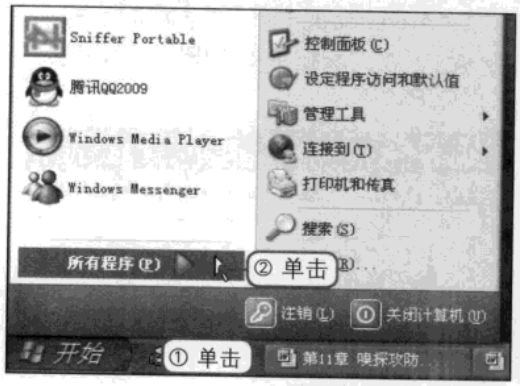
Sniffer Portable是分析网络协议的一个软件，支持各种平台，性能优越，管理人员可以轻松地维护整个网络，监视网络的安全运行情况。

Sniffer Portable在业界有“看不见的网关专家”之称，用它来监控网络以确保网络的正常持续运转，同时可避免网络停机造成的巨大损失。该软件提供了可以快速识别并解决网络性能问题的便携式分析解决方案，并帮助网络技术人员解决所有的局域网和广域网拓扑结构中最困难的问题。Sniffer Portable具有捕捉网络流量进行详细分析、利用专家分析系统诊断问题、实时监控网络活动、手机网络利用率和错误等功能。

由于Sniffer Portable安装后并不在桌面出现对应的快捷方式，因此需要从“开始”菜单中启动，启动后可先设置捕获条件，接着便可捕获报文。

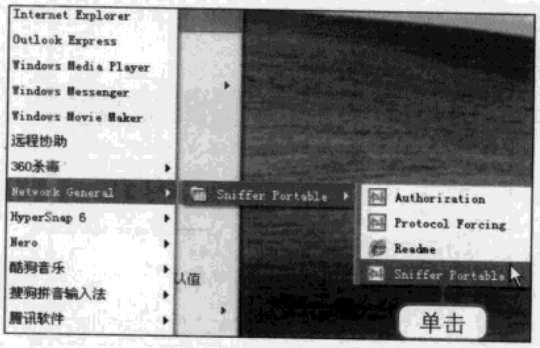
① 单击“所有程序”命令

①在桌面上单击“开始”按钮。②在弹出的菜单中单击“所有程序”命令。



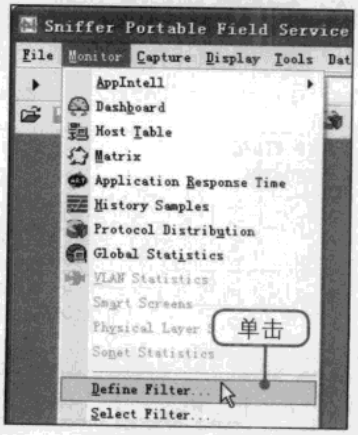
② 启动Sniffer Portable

在右侧弹出的菜单中单击“Network General>Sniffer Portable>Sniffer Portable”命令，启动Sniffer Portable。



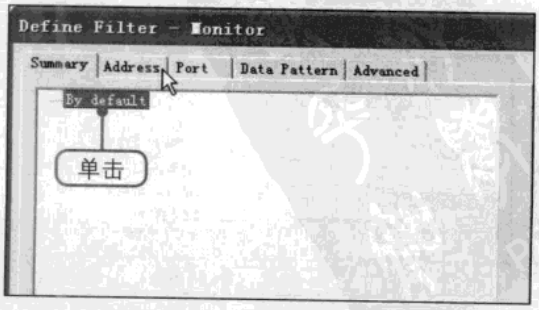
③ 单击Define Filter命令

在主界面窗口单击菜单栏中的Monitor>Define Filter命令。



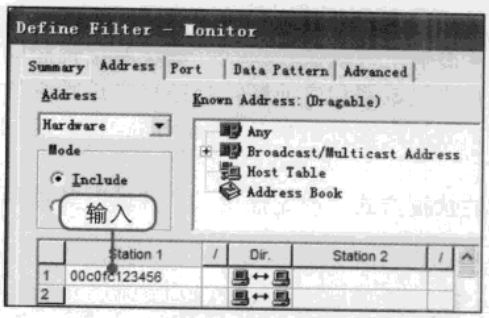
④ 切换至Address选项卡

打开Define Filter-Monitor对话框，单击Address标签切换至该选项卡。



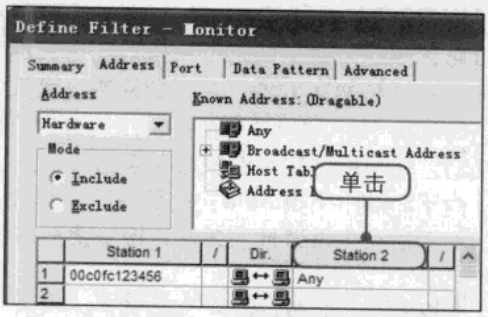
⑤ 设置链路层捕获地址条件

在Station1的第一列中单击并输入链路层捕获地址，例如输入00c0fc123456。



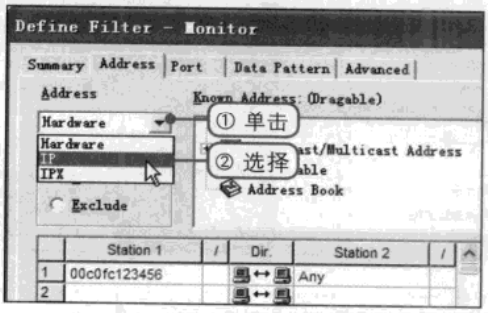
⑥ 默认Station2的设置

单击Station2按钮，此时Station2第一列的地址默认为Any。



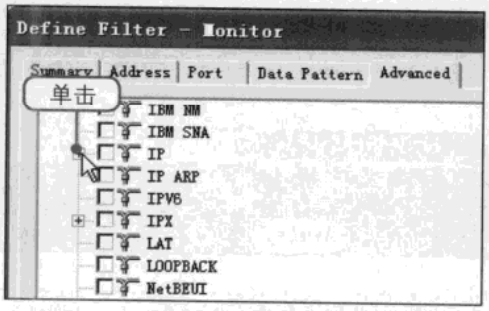
⑦ 设置Address选项

①单击Address下拉列表框右侧的下三角按钮。②在弹出的下拉列表中选择“IP”选项。



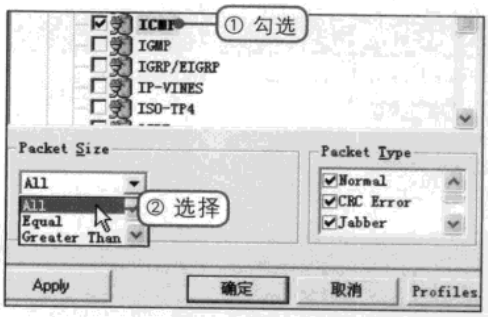
⑧ 展开IP选项

单击Advanced标签切换至该选项卡，向下拖动滑块，在列表框中单击IP选项前的展开按钮，展开IP选项。



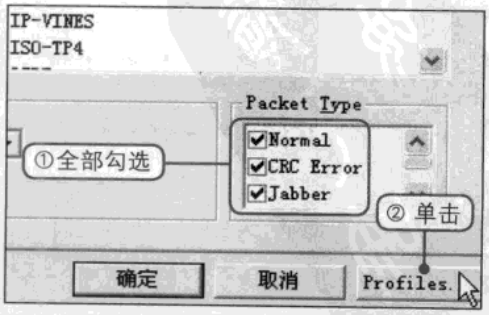
⑨ 设置捕获帧的长度

①勾选 ICMP 复选框。②在“Packer Size”下拉列表中选择捕获帧的长度，例如选择 All 选项。



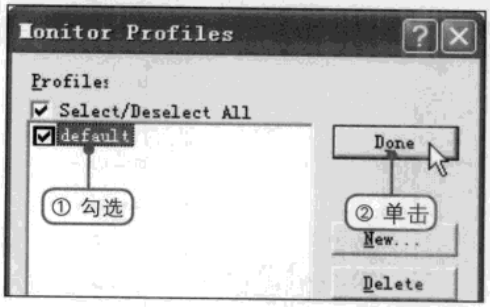
⑩ 设置捕获错误帧

①在 Packet Type 选项组中设置是否捕获错误帧，例如勾选全部的复选框。②单击 Profiles 按钮。



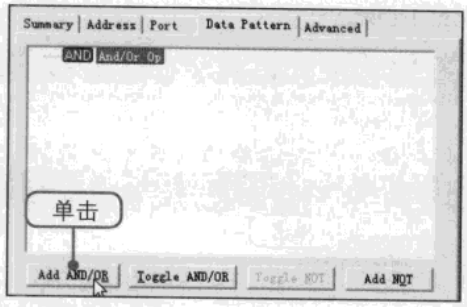
⑪ 保存过滤规则条件

弹出Monitor Profiles对话框，①勾选default复选框。②单击Done按钮，返回Define Filter-Monitor对话框。



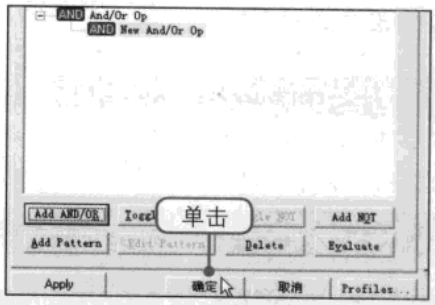
⑫ 编辑任意捕获条件

单击Data Pattern标签切换至该选项卡，用户可在该选项卡下编辑任意捕获条件，例如单击“Add AND/OR”按钮。



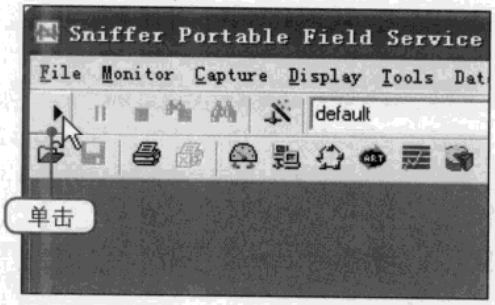
⑬ 单击“确定”按钮

此时可在列表框中看见添加的关系节点，单击“确定”按钮保存退出。



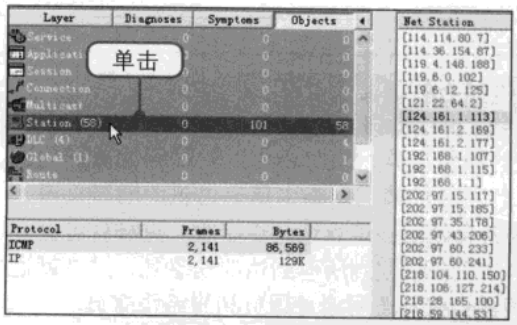
⑭ 开始捕获

返回主界面窗口，在工具栏中单击“开始”按钮开始捕获报文。



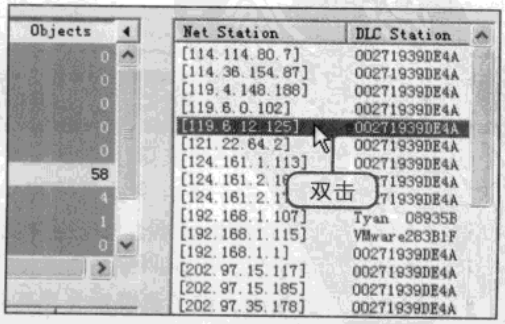
⑮ 选择Station选项

打开Expert窗口，此时可在窗口右侧的Summary选项卡中查看其详细信息并选择窗口左侧的Station选项。



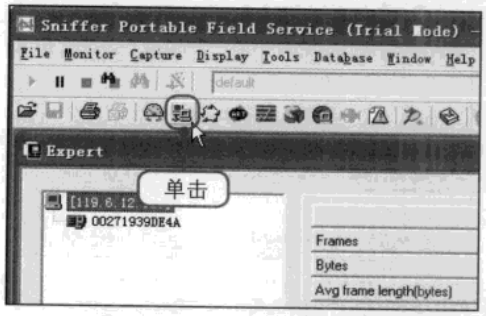
⑯ 双击需要查看的选项

在窗口右侧的列表框中双击需要查看的选项。例如双击119.6.12.125。



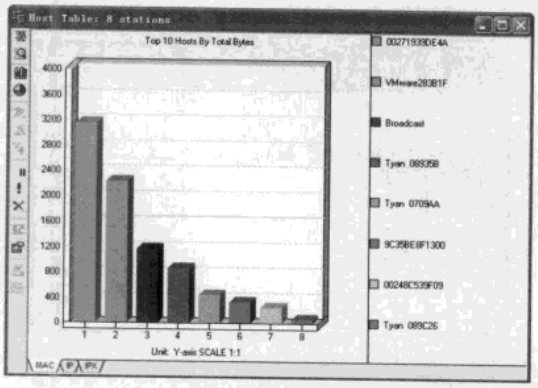
⑰ 查看报文详细信息

此时用户可在Objects选项卡中进一步查看报文，对于某项统计分析可以用鼠标双击此条记录查看详情。接着单击主界面窗口工具栏中的Host Table按钮。



⑱ 查看Host Table报文统计

弹出Host Table对话框，此时可在对话框中看见报文的相关统计信息。

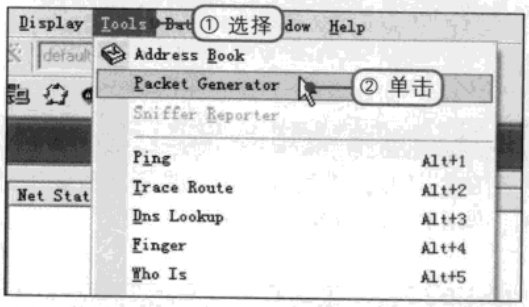


11.2.3 使用Sniffer Portable编辑并发送报文

Sniffer Portable软件除了能够捕获报文之外，还能够编辑并发送报文。

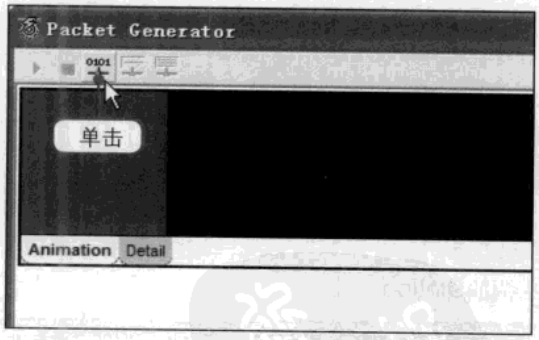
① 打开Packet Generator窗口

①在主界面窗口的菜单栏中选择Tools选项。②在弹出的菜单中单击Packet Generator命令。



② 打开Send new frame对话框

打开Packet Generator窗口，在工具栏中单击0101按钮以打开Send new frame对话框。



Sniffer工作原理

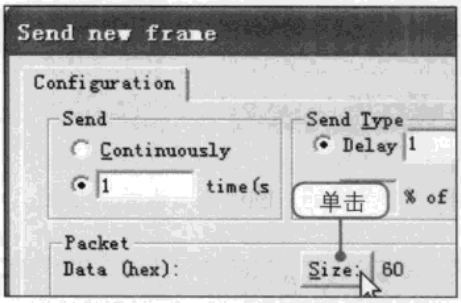
Sniffer工具实际上就是一个网络上的抓包工具，同时还可以对抓到的数据包进行分析。由于在共享式的网络中，信息包是会广播到网络中所有主机的网络接口，只不过在没有使用Sniffer工具之前，主机的网络设备会判断该信息包是否接收，这样就会抛弃不应该接收的信息包，而Sniffer工具能使主机的网络设备接收到所有到达的信息包，这样就达到了网络监听的效果。该工具既适合黑客使用，同样也有利于网络管理员和网络程序员。

拓扑结构

计算机网络的拓扑结构是指网络中各个站点相互连接的形式，在局域网中则表现为文件服务器、工作站（连接在网络上的计算机、大容量的外存、高速打印机等设备均可看作是网络上的一个节点，也称工作站）和电缆等连接形式。现在主要的拓扑结构有总线型拓扑、星型拓扑、环形拓扑以及它们的混合型。

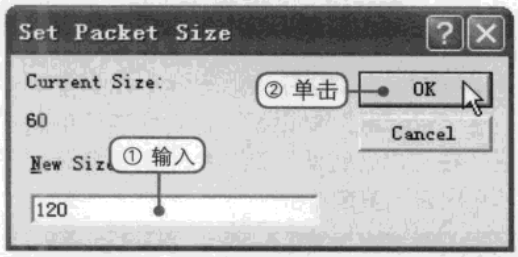
③ 设置发送模式和发送间隔

保持Send和Send Type选项组的默认设置，接着单击下方的Size按钮。



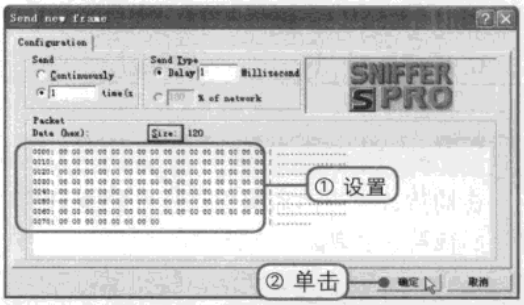
④ 设置数据帧的长度

弹出Set Packet Size对话框，①在New Size文本框中输入设置的数据帧长度。②单击OK按钮。



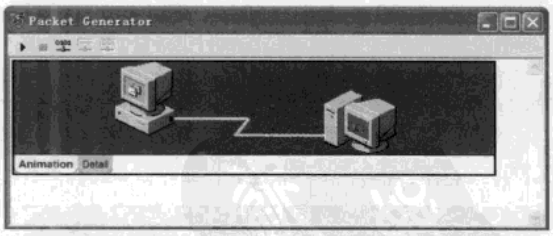
⑤ 编辑报文

返回Send new frame对话框，①在Packet选项组的文本框中调整光标所在的位置，然后对报文进行编辑。②完成后单击“确定”按钮。



⑥ 发送报文

返回Packet Generator窗口，此时可以在窗口中看见报文的发送状态。



11.2.4 使用艾菲网页侦探捕获网页内容

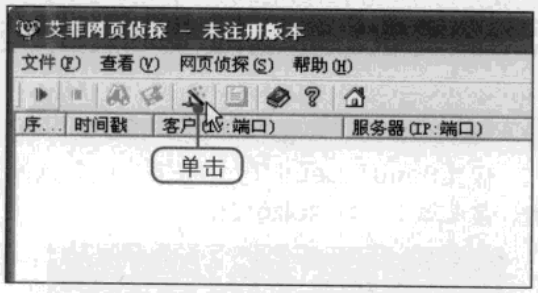
艾菲网页侦探是一个HTTP协议的网络嗅探器、协议分析器和HTTP文件重建工具。它可以捕捉局域网内含有HTTP协议的IP数据包并对其进行分析，找出符合过滤器的HTTP通信内容。用户可通过艾菲网页侦探看到网络中的其他人浏览的网站以及详细内容，该工具特别适用于企业主管对公司员工上网情况进行监控。

① 启动艾菲网页侦探

用户下载并安装好艾菲网页侦探软件之后会在桌面上出现一个对应的快捷图标，双击该图标，启动艾菲网页侦探。

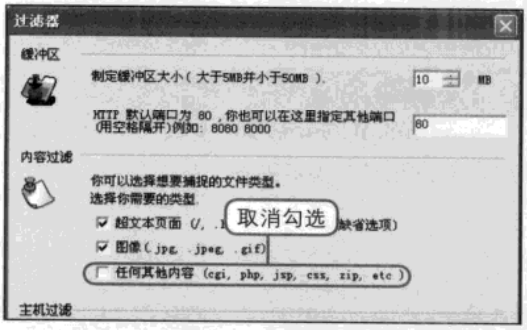
② 打开“过滤器”对话框

打开艾菲网页侦探主界面窗口，单击其工具栏中的“配置捕捉过滤器”按钮，打开“过滤器”对话框。



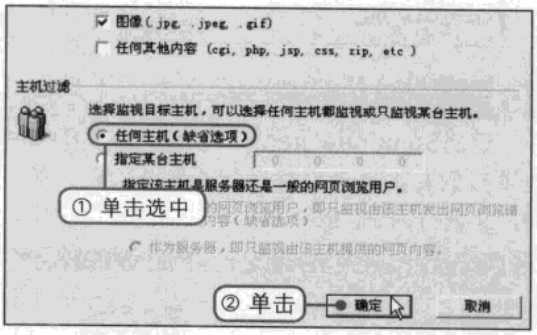
③ 设置内容过滤

在“过滤器”对话框中保持缓冲区的默认设置，在“内容过滤”选项组中取消勾选“任何其他内容”复选框。



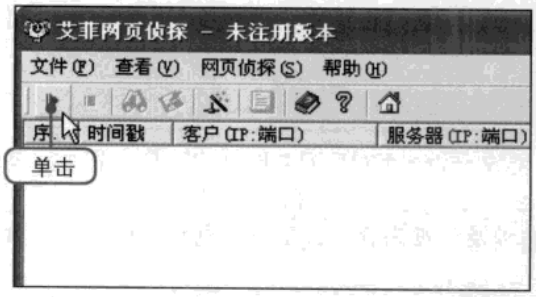
④ 设置主机过滤

①在“主机过滤”选项组中单击选中“任何主机”单选按钮。②单击“确定”按钮。



⑤ 开始捕获网页

返回艾菲网页侦探主界面窗口，在窗口的工具栏中单击“开始”按钮开始捕获网页。



⑥ 查看捕获的内容

在捕获过程中艾菲网页侦探会把捕获的内容显示在其主页面的文本框中。

11.3 → 防范Sniffer

网络监听一直是网络安全中比较突出的问题，它作为一种发展比较成熟的技术，在协助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用，一直被广大的网络管理员所使用。然而许多网络入侵往往都伴随着网络监听行为，从而造成密码丢失、重要数据被截获等，因此用户需要防范嗅探攻击。

一般在网络中很难发现Sniffer，因为它根本就不会留下任何痕迹，但是用户可以通过查看进程的方法来发现Sniffer的存在。在Windows操作系统中可右击任务栏的空白处，然后在弹出的快捷菜单中单击“任务管理器”命令打开Windows“任务管理器”窗口，在任务管理器中即可查看进程列表。有两种防范Sniffer的方法供用户使用。

1 传输加密

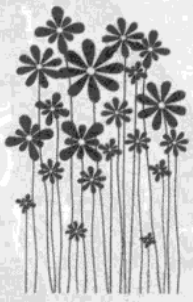
传输加密是指在传输数据之前先对该数据进行加密操作，当对方接收到数据之后再解密。这样一来即使被Sniffer监听并截获，但它看到的仅仅是加密后的数据，没有密码也无法打开该文件。由于传统的TCP/IP协议并没有采用加密的方法进行数据的传输，数据的传输都是通过明文方式进行的，因此想要彻底地解决被Sniffer监听，最根本的方法就是增强TCP/IP协议，而目前只能通过打补丁来解决。

2 采用安全拓扑结构

采用安全拓扑结构要遵循的一个原则就是一个网络段必须有足够的理由才能相信另外一个网络段，网络段的设计要考虑数据之间的信任关系，而不是硬件关系。

无论是采用传输加密，还是采用安全拓扑结构，由于Sniffer程序一般是入侵者在入侵系统之后才会使用它来收集有用的信息，因此防范系统被入侵才是解决问题的关键，系统管理员要定期地对所管理的网络进行安全测试，以便即时地防范和防止安全隐患。

读书笔记



Chapter 12

远程控制

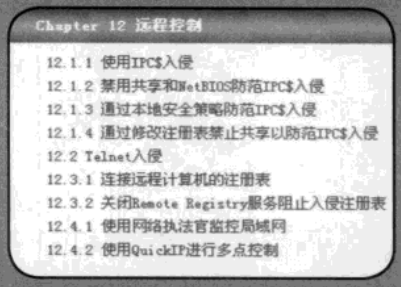
重点知识

1. IPC$入侵与防范
2. Telnet入侵
3. 通过注册表入侵
4. 远程监控

远程控制是指在网络上由一台电脑（主控端/客户端）远距离去控制另一台电脑（被控端/服务器端）的技术。黑客们通过远程控制取得目标电脑的管理员权限，然后窃取目标电脑中的重要资料和数据，除此之外，黑客还可能对目标文件进行操作、修改注册表、监视其屏幕的一举一动，甚至可以实时地控制远程计算机用户的操作。

视频文件

参见随书光盘：视频教程\Chapter 12



12.1 IPC$入侵与防范

IPC$是Windows系统特有的一项管理功能，是为了方便用户使用电脑而设计的。IPC$主要用于远程管理计算机，但是这个特点也给入侵者以可乘之机，入侵者可以通过建立IPC$连接来实现对远程主机的通信和控制。

12.1.1 使用IPC$入侵

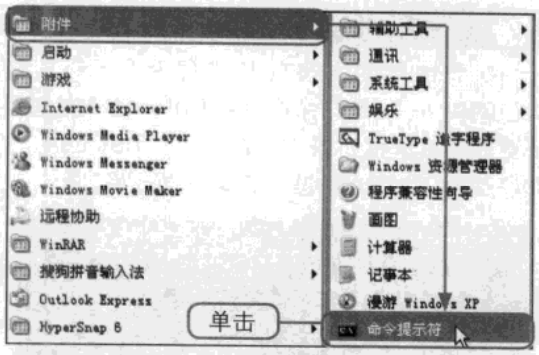
使用IPC$入侵首先要获得目标主机的管理员账号和密码，然后便可建立IPC$连接，进而将远程磁盘映射到本地计算机中。

① 单击“所有程序”命令

①在桌面上单击“开始”按钮，弹出“开始”菜单，②在“开始”菜单中单击“所有程序”命令。

② 打开“命令提示符”窗口

在右侧弹出的菜单中单击“附件>命令提示符”命令，打开“命令提示符”窗口。

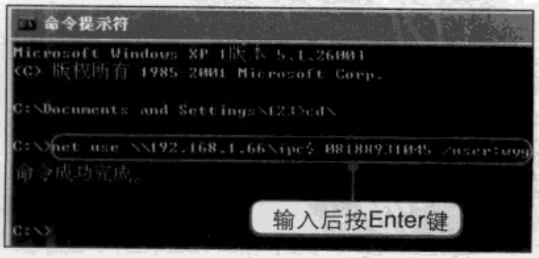


③ 输入cd\命令

在“命令提示符”窗口中输入cd\命令后按Enter键，将当前目录更改至C盘根目录下。

④ 建立IPC$连接

建立IPC$连接的命令格式为：net use \\IP\ipc$ Passwd/user:Admin。其中IP表示目标电脑的IP地址，Passwd表示目标电脑的密码，Admin表示目标电脑的用户名。

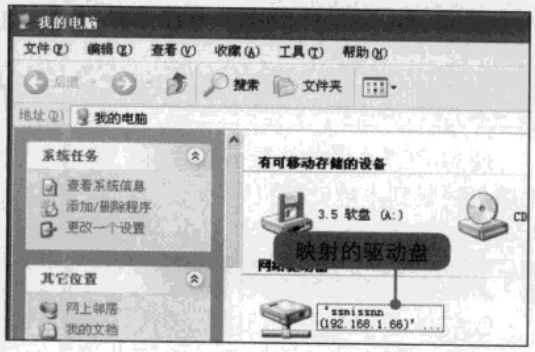


⑤ 建立映射

建立映射命令的格式为：net use z: \\IP\c$，其中\\IP\c$表示目标电脑上的C盘，符号“$”表示隐藏的共享，“z:”表示将远程主机的C盘映射为本地磁盘的盘符。

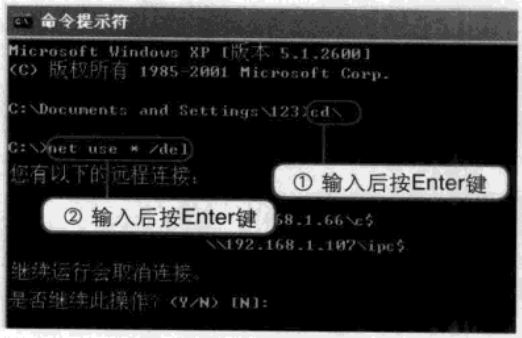
⑥ 映射成功

映射成功之后打开“我的电脑”窗口，在“网络驱动器”选项组下可以看见“ssmissnn (192.168.1.66)上的C$”盘符。在该盘符中可进行复制、剪切等操作。



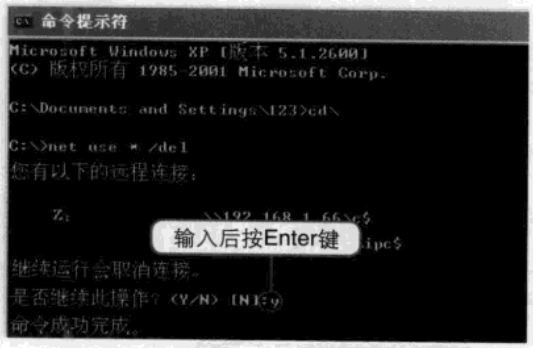
⑦ 查看远程连接

按照前面的方法打开“命令提示符”窗口，①输入“cd\”命令后按Enter键将当前目录更改至C盘根目录下。②输入“net use * /del”命令后按Enter键，查看远程连接。



⑧ 断开连接

光标固定在“是否继续此操作”选项右侧，输入“y”后按 Enter 键即可断开这些连接。



IPC$空连接漏洞

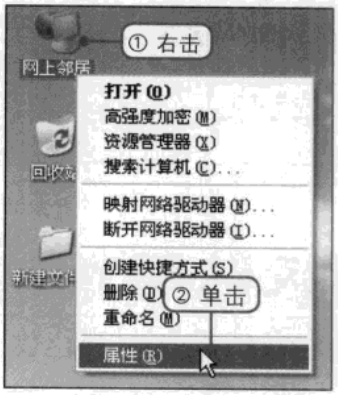
IPC$连接原本是要求客户机具有足够的权限才能连接到主机，然而IPC$连接漏洞允许客户端只使用空用户名和密码就可以与目标主机成功地建立连接。入侵者利用该漏洞进入目标主机之后，虽然无法执行管理类操作，即不能映射网络驱动器、上传文件、执行脚本等命令，但是却可以用来探测目标主机中的一些信息。

12.1.2 禁用共享和NetBIOS防范IPC$入侵

可以在命令提示符中输入net share命令来查看本机上是否存在共享，若存在则很有可能被入侵者抓住IPC$漏洞对该电脑进行攻击。

① 打开“网络连接”窗口

①右击桌面上的“网上邻居”快捷图标。②在弹出的快捷菜单中单击“属性”命令。

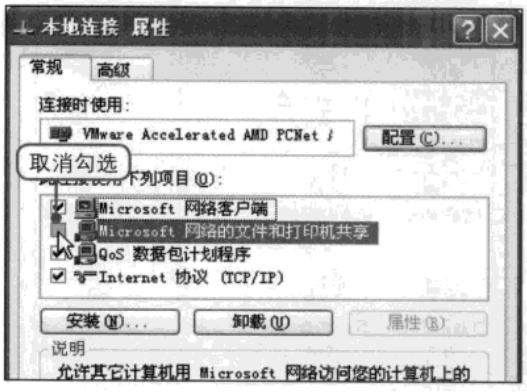


② 选择“属性”命令

打开“网络连接”窗口，①右击“本地连接”图标。②在弹出的快捷菜单中单击“属性”命令。

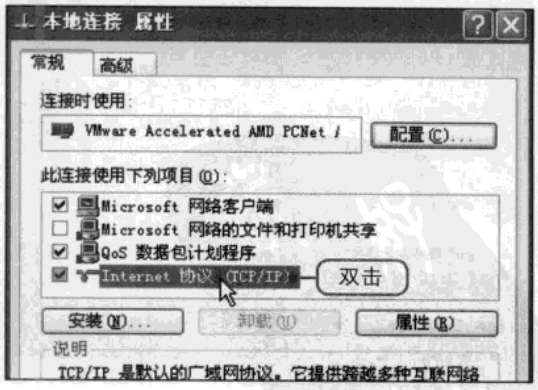
③ 禁用文件和打印机共享

打开“本地连接 属性”对话框，在常规选项卡中取消勾选“Microsoft 网络的文件和打印机共享”复选框。



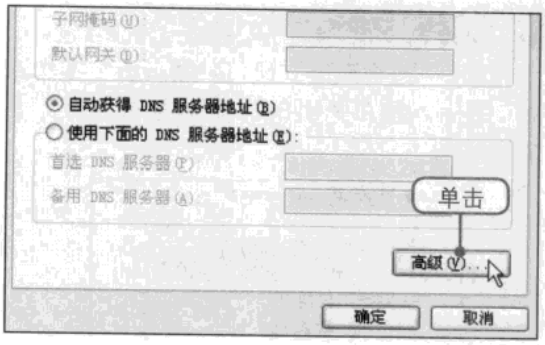
④ 双击“Internet协议”选项

双击“Internet协议（TCP/IP）”选项，打开“Internet协议（TCP/IP）属性”对话框。



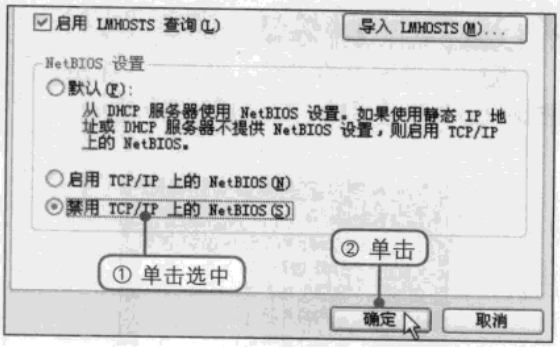
⑤ 打开“高级TCP/IP设置”对话框

在对话框中单击下方的“高级”按钮，打开“高级TCP/IP设置”对话框。



⑥ 禁用TCP/IP上的NetBIOS

单击“WINS”标签切换至该选项卡下，①单击选中“禁用TCP/IP上的NetBIOS”单选按钮。②单击“确定”按钮保存退出。

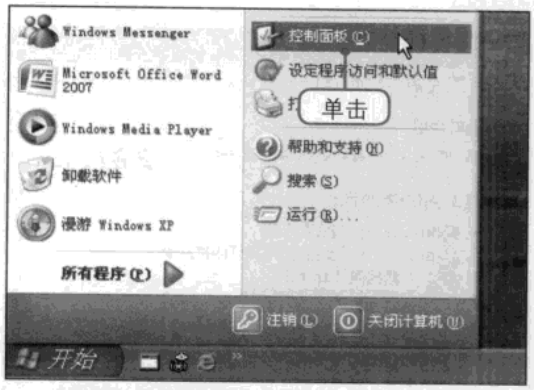


12.1.3 通过本地安全策略防范IPC$入侵

可以通过在本地安全设置中开启允许SAM账户和共享的匿名枚举来防范IPC$的入侵。

① 打开“控制面板”窗口

单击桌面上的“开始”按钮，在弹出的“开始”菜单中单击“控制面板”命令，打开“控制面板”窗口。

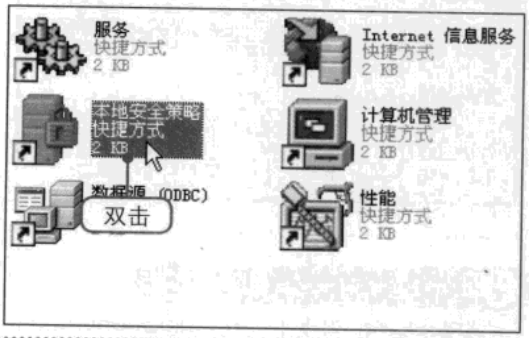


② 打开“管理工具”窗口

在“控制面板”窗口中双击“管理工具”图标，打开“管理工具”窗口。

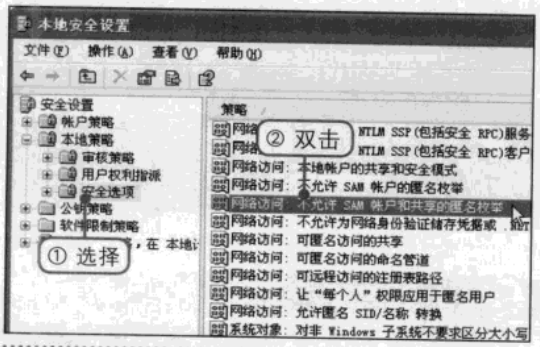
③ 打开“本地安全设置”窗口

在“管理工具”窗口中双击“本地安全策略”图标，打开“本地安全设置”窗口。



④ 禁用TCP/IP上的NetBIOS

①在“本地安全设置”窗口的左侧选择“安全设置>本地策略>安全选项”选项，②在窗口的右侧双击“网络访问：不允许SAM账户和共享的匿名枚举”选项。

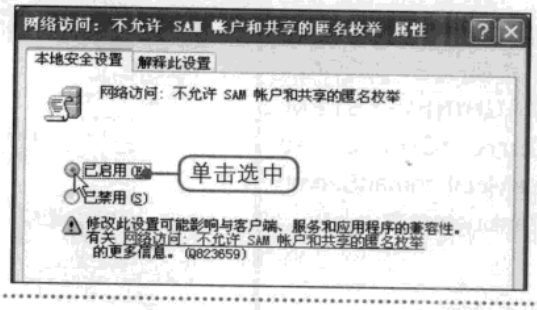


SAM账户

SAM是Security Accounts Manager的缩写，中文译为安全性账户管理员。SAM文件记录了电脑中所有用户的用户名和密码，这样在登录的时候用户才可以使用不同的用户名登录到本地电脑。如果用户忘记密码，则可以在DOS下删除SAM文件，然后用Administrator的空密码账户登录本地电脑。

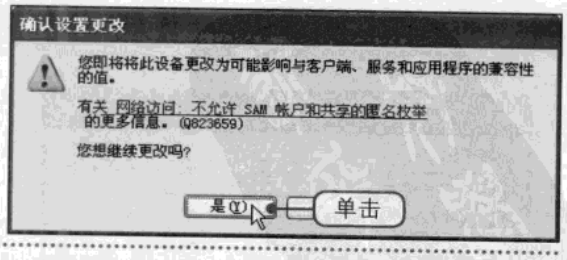
⑤ 关闭共享

在弹出的对话框中单击选中“已启用”单选按钮，即开启不允许SAM账户和共享的匿名枚举服务。



⑥ 确认关闭共享

单击“确定”按钮后弹出“确认设置更改”提示框，单击“是”按钮保存退出即可。



12.1.4 通过修改注册表禁止共享以防范IPC$入侵

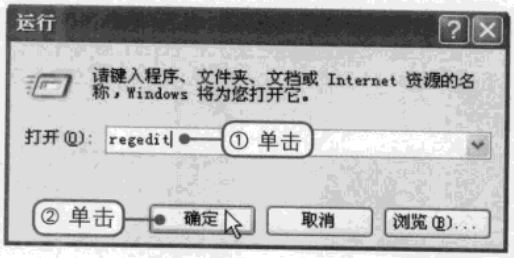
用户也可以在注册表中设置禁止共享来防范IPC$的入侵，只是在设置时有服务器和客户机之分。

① 打开“运行”对话框

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“运行”命令，打开“运行”对话框。

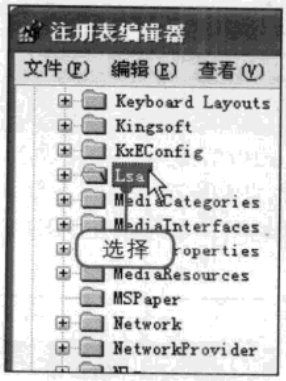
② 打开“注册表编辑器”窗口

①在“打开”文本框中输入regedit命令。②单击“确定”按钮，打开“注册表编辑器”窗口。



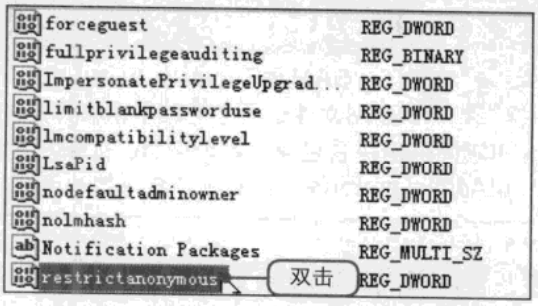
③ 查找Lsa子项

在窗口的左侧选择HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa分支。



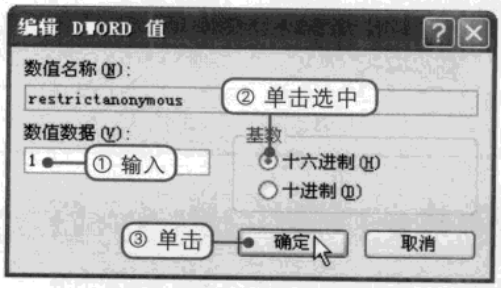
④ 打开编辑键值项对话框

在窗口的右侧双击“restrictanonymous”键值项，打开编辑DWORD值对话框。



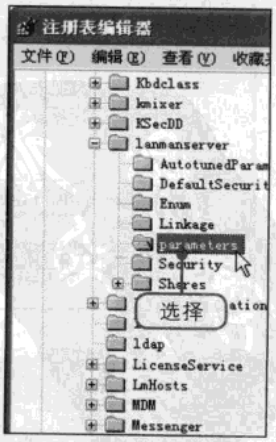
⑤ 设置数值数据

①在“数据数值”文本框中输入1。②在“基数”选项组中单击选中“十六进制”单选按钮。③单击“确定”按钮。



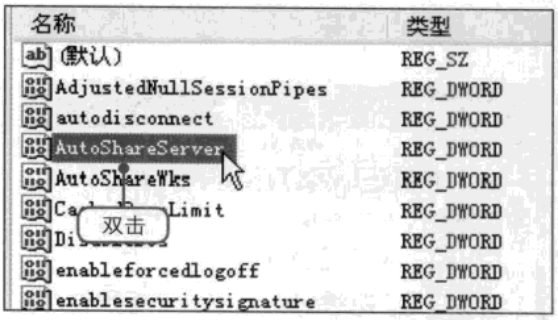
⑥ 确认关闭共享

返回“注册表编辑器”窗口，在左侧窗格中选择HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\LanmanServer\Parameters选项。



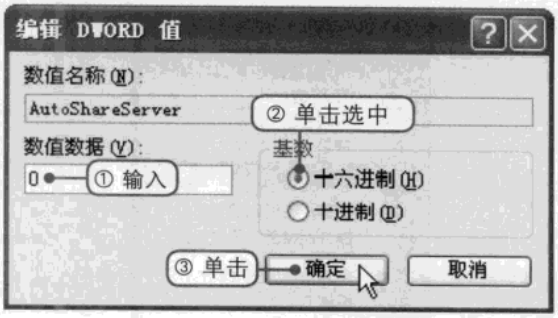
⑦ 打开编辑键值项对话框

如果该电脑充当的是服务器，则在窗口的右侧双击AutoShareServer键值项，打开“编辑 DWORD 值”对话框。



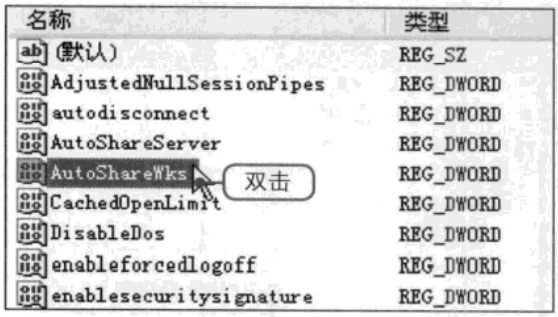
⑧ 编辑键值项

①在“数值数据”文本框中输入0。②在“基数”选项组中单击选中“十六进制”单选按钮。③单击“确定”按钮。



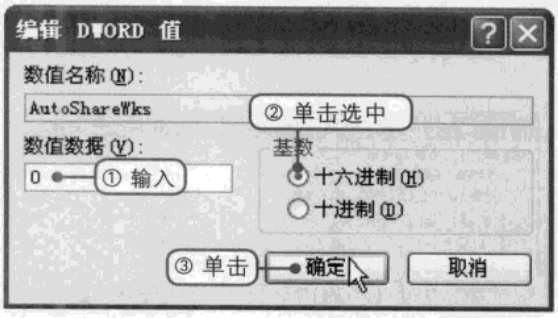
⑨ 打开编辑键值项对话框

如果该电脑是充当客户机，则在窗口的右侧双击AutoShareWks键值项，打开“编辑 DWORD 值”对话框。



⑩ 编辑键值项

①在“数值数据”文本框中输入0。②在“基数”选项组中单击选中“十六进制”单选按钮。③单击“确定”按钮即可。



12.2 Telnet入侵

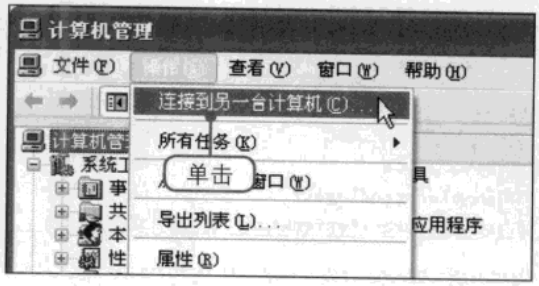
Telnet入侵与真正的登录有着不同的地方，使用Telnet入侵只是与远程主机建立了连接，实际上它是夺取远程主机的控制权后登录，而这也正是黑客们使用Telnet入侵的真正目的。

① 打开“计算机管理窗口”

①右击桌面上“我的电脑”快捷图标，②在弹出的快捷菜单中单击“管理”命令，打开“计算机管理”窗口。

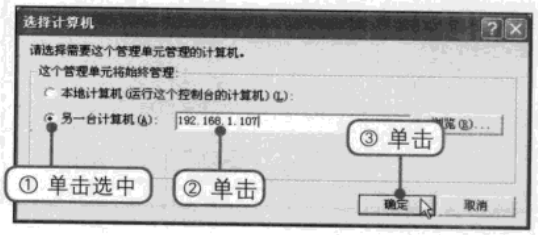
② 打开“选择计算机”对话框

单击菜单栏中的“操作>连接到另一台计算机”命令，打开“选择计算机”对话框。



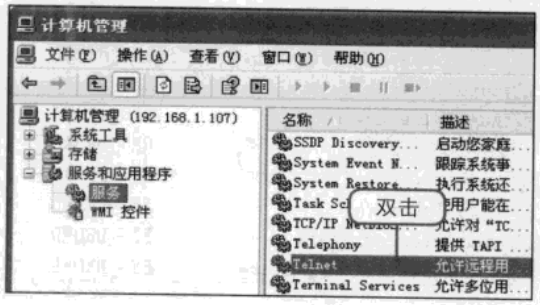
③ 输入远程计算机的IP地址

①在对话框中单击选中“另一台计算机”单选按钮。②在文本框中输入192.168.1.107。③单击“确定”按钮。



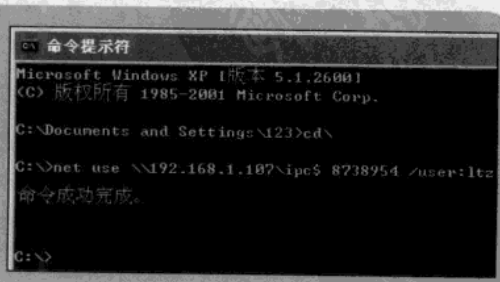
④ 打开“Telnet的属性”对话框

返回“计算机管理”窗口，用户可在计算机管理目录中看见远程计算机的IP地址。接着在“服务”选项卡中双击Telnet选项。



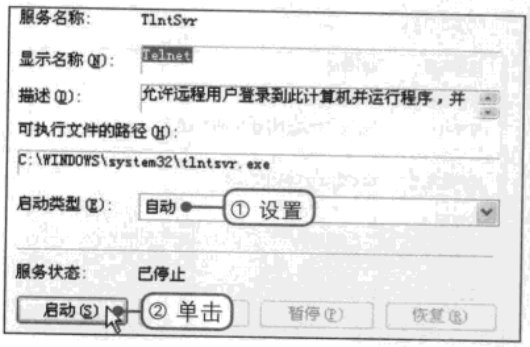
使用Telnet入侵前须建立IPC$连接

使用Telnet入侵前需要建立IPC$连接，可参照前面介绍的方法建立IPC$连接。建立IPC$连接是为了方便开启远程计算机中被禁用的Telnet服务，接着就可以利用IPC$连接来开启远程计算机的Telnet服务。



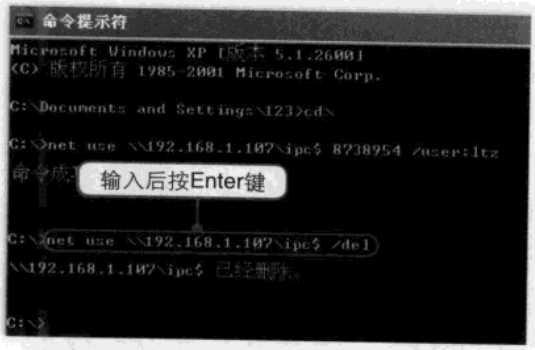
⑤ 启动Telnet服务

打开“Telnet的属性”对话框，①设置启动类型为自动。②单击“启动”按钮。



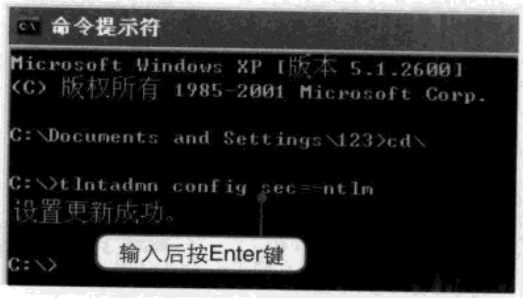
⑥ 断开IPC$连接

在“命令提示符”窗口中输入net use \\IP\ipc$/del命令来断开IPC$连接。



⑦ 去掉NTLM验证

再次打开“命令提示符”窗口，更改目录至C盘根目录下，输入tlntadmn config sec = -ntlm命令后按Enter键。

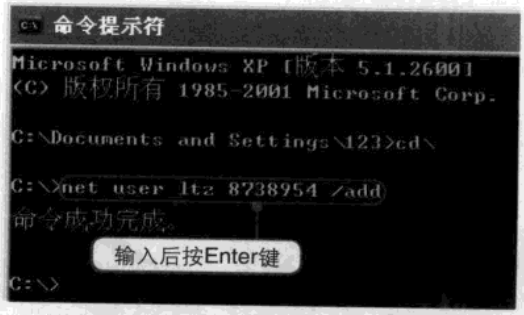


去掉NTLM验证的原因

前面介绍过若使用Telnet入侵，则需要通过建立IPC$连接开启远程计算机上的Telnet服务，同时需要去掉NTLM验证，若用户在没有去掉NTLM验证的状态下登录远程计算机，则会直接导致登录失败。

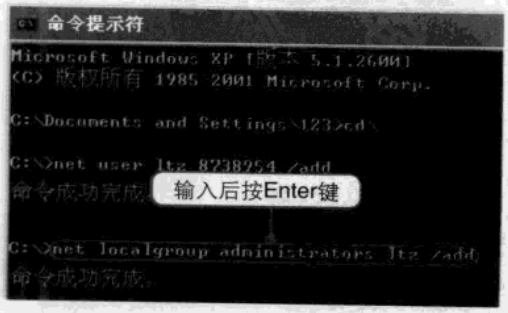
⑧ 建立账号和密码

在“命令提示符”窗口中输入net user Admin passwd/add命令后按Enter键。



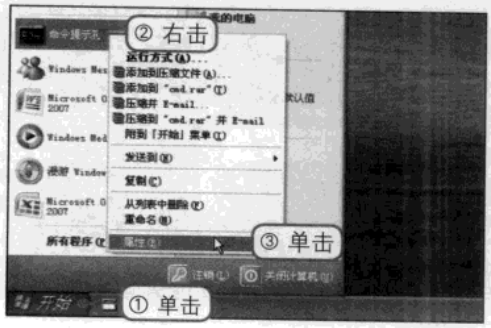
⑨ 加入工作组

在“命令提示符”窗口中输入net localgroup administrators ltz/add命令后按Enter键。



⑩ 打开“命令提示符属性”对话框

①单击桌面上的“开始”按钮。②在“开始”菜单中右击“命令提示符”选项。③在弹出的快捷菜单中单击“属性”命令。

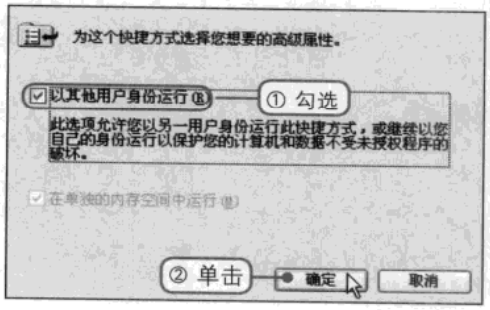


⑪ 打开“高级属性”对话框

打开“命令提示符属性”对话框，在对话框中单击下方的“高级”按钮，打开“高级属性”对话框。

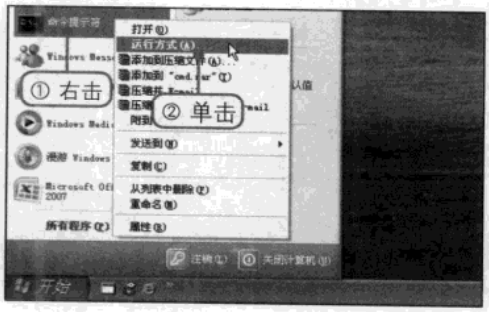
⑫ 设置高级属性

①在对话框中勾选“以其他用户身份运行”复选框。②单击“确定”按钮。



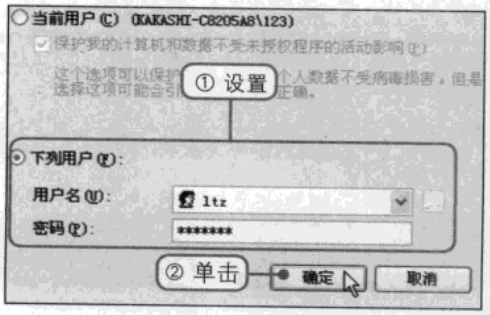
⑬ 打开“运行身份”对话框

①右击“命令提示符”选项。②在弹出的快捷菜单中单击“运行方式”命令。



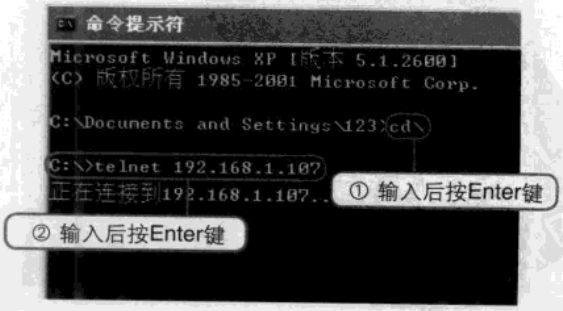
⑭ 设置运行身份

①单击选中“下列用户”单选按钮并输入用户名和密码。②单击“确定”按钮。



⑮ 进行Telnet登录

①在“命令提示符”窗口中切换至C盘根目录下。②输入telnet IP后按Enter键。



12.3 通过注册表入侵

Windows注册表是帮助Windows控制硬件、软件、用户环境和Windows界面的一套数据文件，入侵者可在注册表编辑器中通过连接网络注册表进入远程计算机的注册表并进行实时监控。用户若想阻止该类入侵，只需禁用Remote Registry服务。

12.3.1 连接远程计算机的注册表

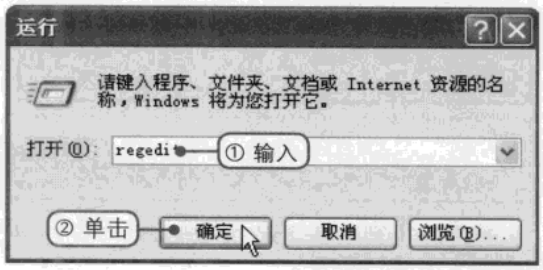
微软公司出于方便网络管理员对网络中电脑进行管理的目的，在注册表编辑器中设置了连接网络注册表功能，这样管理员和用户通过注册表就可以在网络上检查系统的配置和设置，实现远程管理。但是该功能却被黑客所利用，进入他人的注册表并对注册表进行远程操作。

① 打开“运行”对话框

①单击桌面上的“开始”按钮。②在弹出的“开始”菜单中单击“运行”命令，打开“运行”对话框。

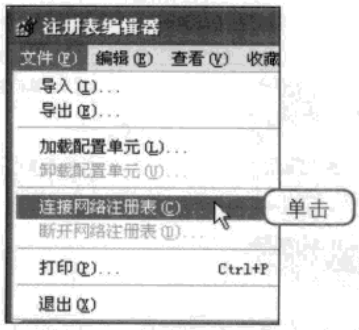
② 打开“注册表编辑器”窗口

①在“打开”文本框中输入regedit命令。②单击“确定”按钮，打开“注册表编辑器”窗口。



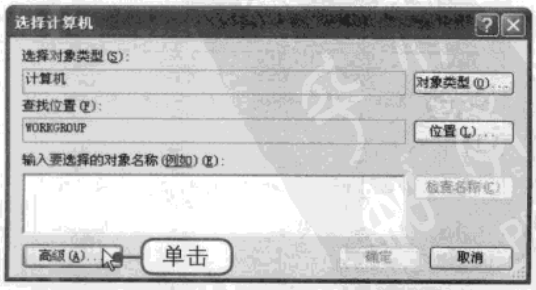
③ 单击“连接网络注册表”命令

单击“文件>连接网络注册表”命令。



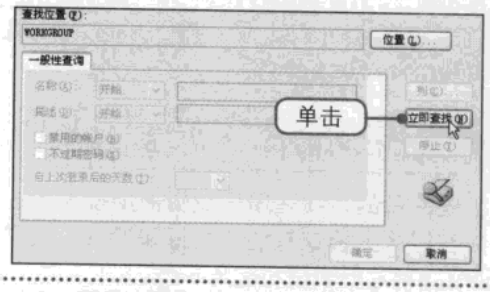
④ 单击“高级”按钮

打开“选择计算机”对话框，在对话框底部单击“高级”按钮。



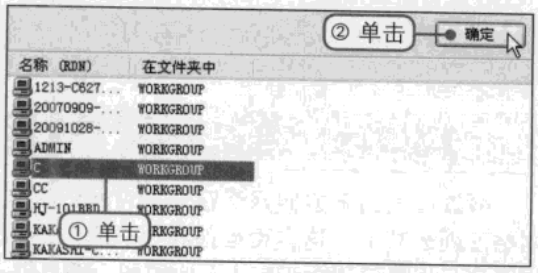
⑤ 查找远程计算机

在“一般性查询”选项卡中单击“立即查询”按钮。



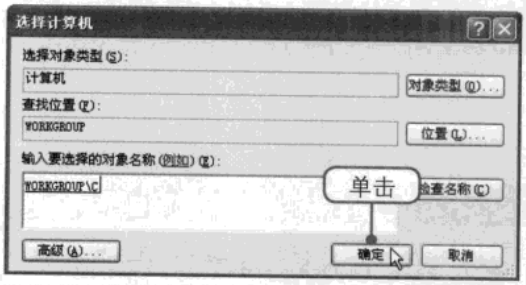
⑥ 选择远程计算机

①在查找结果中单击一台计算机。②单击“确定”按钮。



⑦ 连接远程计算机

将远程计算机添加到文本框之后，单击“确定”按钮连接计算机。



⑧ 连接成功

连接成功后，用户可在“注册表编辑器”窗口左侧的窗格下看见远程计算机的注册表。

12.3.2 关闭Remote Registry服务阻止入侵注册表

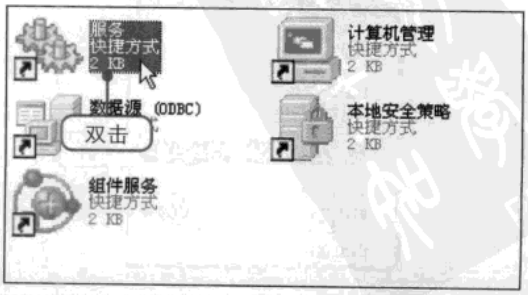
若想阻止别人远程控制电脑的注册表，则可在“服务”窗口中关闭Remote Registry服务即可阻止别人入侵注册表。

① 打开“管理工具”对话框

在桌面上单击“开始>控制面板”命令打开“控制面板”窗口，接着在窗口中双击“管理工具”图标。

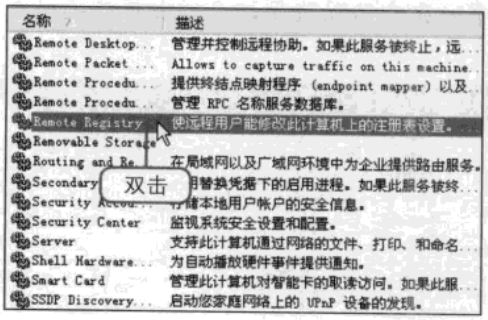
② 打开“服务”窗口

打开“管理工具”窗口，接着在窗口中双击“服务”图标，打开“服务”窗口。



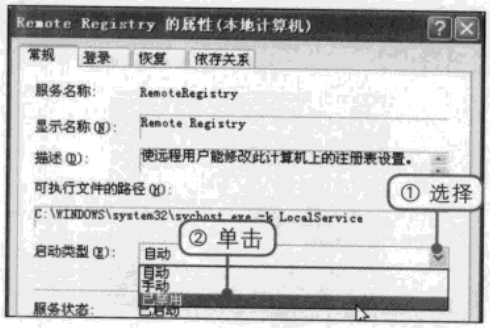
③ 打开“Remote Registry属性”对话框

在“服务”窗口中双击Remote Registry选项，打开“Remote Registry的属性”对话框。



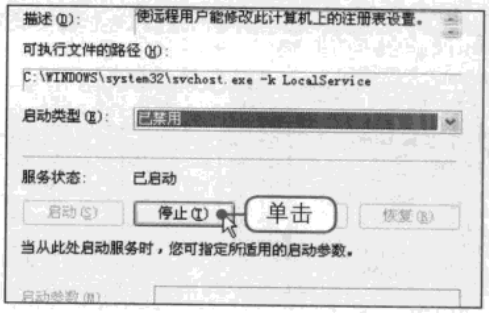
④ 设置启动类型为已禁用

①在弹出的对话框中单击“启动类型”下拉列表框右侧的下三角按钮。②在弹出的下拉列表中选择“已禁用”选项。



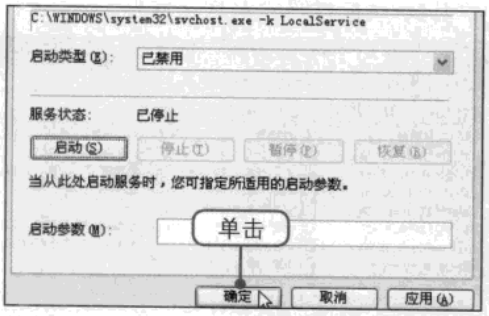
⑤ 设置服务状态为停止

在“服务状态”选项组中单击“停止”按钮，设置服务状态为停止。



⑥ 单击“确定”按钮

设置完毕后单击“确定”按钮保存退出即可。



12.4 远程监控

远程监控，即远程监视和控制。远程监视即对电脑所处的环境以及计算机系统和网络设备的监视，主要是以获取网络信息为主；而远程控制是指通过网络对远程计算机进行日常设置的工作，通过硬件的配合还可以实现远程开机的功能。

12.4.1 使用网络执法官监控局域网

“网络执法官”是一款局域网管理软件，它采用的是网络底层协议，用户只需要在局域网的任意一台电脑上运行即可穿透局域网中其他电脑的用户防火墙，并且对网络中的每一台主机进行监控。同时它采用网卡识别用户，可靠性比同类软件有了很大的提高，另外，软件本身占用的网络资源较少，对网络的运行没有不良的影响。

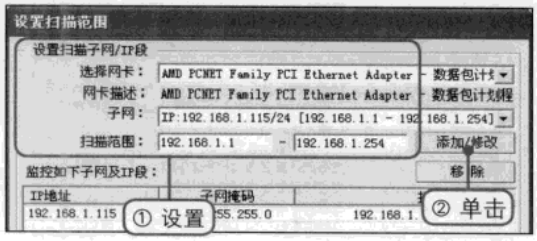
网络执法官的主要功能有：实时记录上线用户并存档备查、自动侦测未登记主机接入并报警、检测网内所有代理服务器及路由器、限定各主机的IP、防止IP盗用等。

① 启动网络执法官

用户下载并安装好网络执法官之后会在桌面上出现对应的快捷图标，双击该图标，启动该应用程序。

② 设置扫描范围

打开“设置扫描范围”对话框，①用户可根据自身的情况选择网卡和设置扫描范围，②单击“添加/修改”按钮添加至列表框。



③ 查看处于监控状态下的计算机

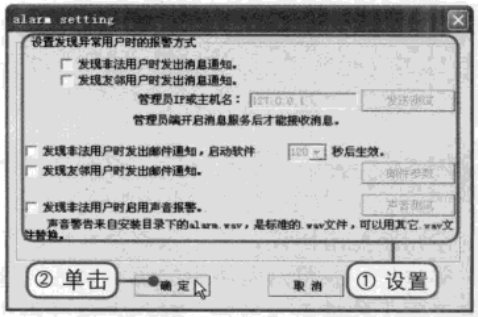
单击“确定”按钮后返回网络执法官主界面窗口，此时可在“本网用户”选项卡下看见设置扫描范围后计算机的相关信息。

④ 打开“报警设置”对话框

在窗口的菜单栏中单击“设置>报警设置”命令，打开alarm setting对话框。

⑤ 设置报警

①用户可根据自己的情况设置发现异常时的报警方式。②单击“确定”按钮。

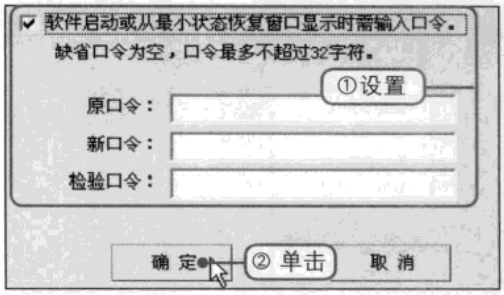


⑥ 打开“设置口令”对话框

返回主界面窗口，单击菜单栏中的“设置>口令”命令。

⑦ 设置口令

打开“设置口令”对话框，①勾选“软件启动或从最小状态恢复窗显示时需输入口令”复选框并在下方输入设置的口令。②单击“确定”按钮。

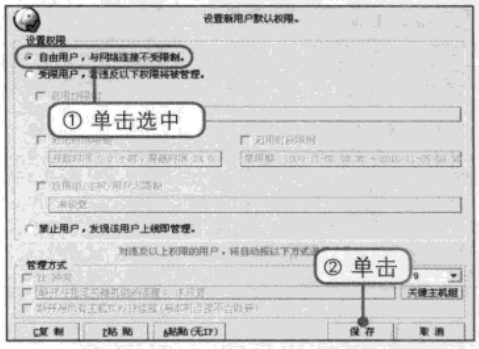


⑧ 打开“用户权限设置”对话框

返回主界面窗口，单击菜单栏中的“设置>默认权限”命令，打开“用户权限设置”对话框。

⑨ 设置用户权限

①在“设置权限”选项组中设置不同的权限，例如单击选中“自由用户，与网络连接不受限制”单选按钮。②单击“保存”按钮。

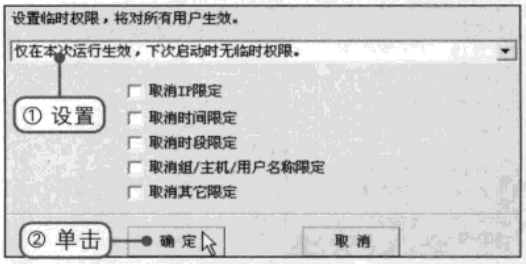


⑩ 打开“临时权限”对话框

返回主界面窗口，单击菜单栏中的“设置>临时权限”命令，打开“临时权限”对话框。

⑪ 设置临时权限

①在对话框中的下拉列表中选择临时权限持续的时间，②设置权限后单击“确定”按钮。



⑫ 打开“关键主机组设置”对话框

返回主界面窗口，单击菜单栏中的“设置>关键主机组”命令，打开“关键主机组”对话框。

⑬ 设置关键主机组

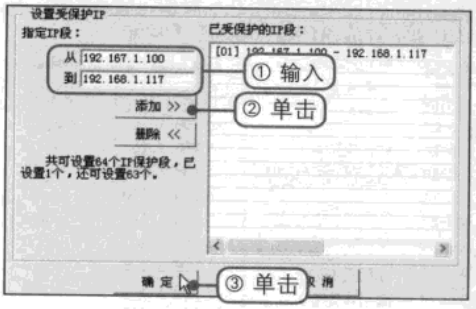
在“选择关键主机组”下拉列表中选择关键主机组并在“组名称”文本框中输入对应的名称，然后单击“全部保存”按钮。

⑭ 打开“IP保护”对话框

返回主界面窗口，单击菜单栏中的“设置>IP保护”命令，打开“IP保护”对话框。

⑮ 设置IP保护

①在“指定IP段”文本框中输入设置的IP地址范围。②单击“添加”按钮。③单击“确定”按钮。

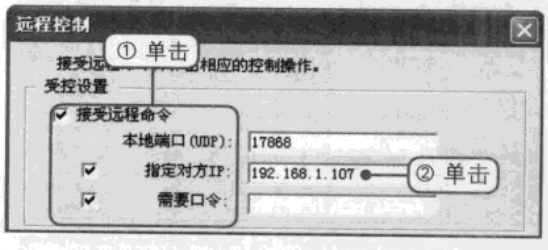


⑯ 打开“远程控制”对话框

返回主界面窗口，单击菜单栏中的“设置>远程控制”命令，打开“远程控制”窗口。

⑰ 设置远程控制

①在“远程控制”对话框中勾选所有的复选框。②并在对应的文本框中输入指定对方的IP及需要口令。

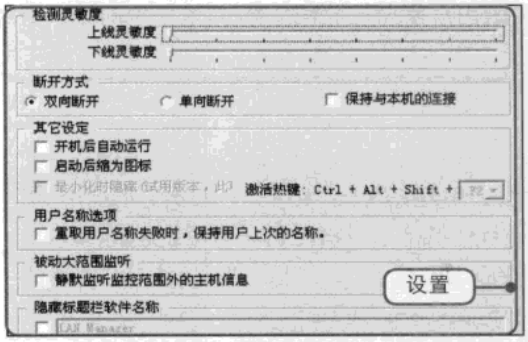


⑱ 打开“其他设定”对话框

返回主界面窗口，单击菜单栏中的“设置>其它设定”命令，打开“其它设定”对话框。

19 其他设置

在对话框中用户可根据自身的情况设置检验的灵敏度、断开方式以及其他的设置，设置完毕后单击“确定”按钮。



20 打开“MAC-IP绑定”对话框

①选中需要绑定MAC-IP的计算机，然后右击。②在弹出的快捷菜单中单击“绑定MAC与IP机器名称”命令。

21 MAC-IP绑定

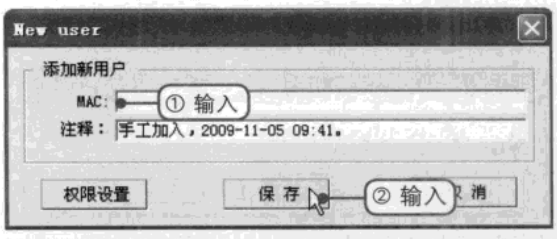
打开“MAC-IP绑定”对话框，绑定MAC与IP的目的是防止多台主机共享一个上网地址，设置后单击“确定”按钮。

22 打开New User对话框

返回主界面窗口，在菜单栏中单击“用户>添加用户”命令，打开New User对话框。

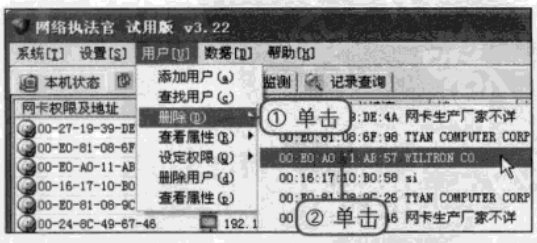
23 添加新用户

①在“添加新用户”选项组中的MAC文本框中输入新用户的MAC地址。②单击“保存”按钮返回主界面窗口。



24 删除用户

若用户想要删除某个用户，①在菜单栏中单击“用户>删除”命令。②在弹出的级联菜单中单击需要删除的用户即可。



新手学堂

MAC地址

MAC（Media Access Control，介质访问控制）地址是烧录在网卡里的，也叫硬件地址，是由48比特长（6字节）的十六进制数字组成。0～23位叫做组织唯一标志符，是识别局域网节点的标识，24～47位则由厂家自己分配。MAC地址如同用户身份证上的身份证号码，具有全球唯一性。

提示

查看电脑的MAC地址

用户可在“命令提示符”窗口中查看该电脑的MAC地址。①打开“运行”对话框，在“打开”文本框中输入cmd。②单击“确定”按钮打开命令提示符窗口。③在窗口中输入“ipconfig/all”命令后按Enter键，“命令提示符”窗口中显示的Physical Address选项就是该电脑的MAC地址。

12.4.2 使用QuickIP进行多点控制

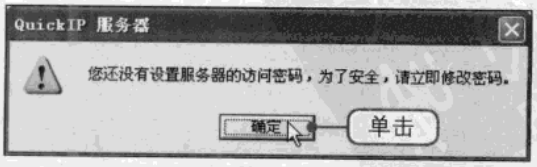
QuickIP是一款基于TCP/IP的计算机远程控制软件，使用该软件可以通过局域网、互联网全权控制远程的计算机，服务器可以被多台客户机控制，而一台客户机也可以同时控制多台服务器。

① 启动QuickIP服务器

用户下载并安装好QuickIP软件之后会在桌面上出现对应的快捷图标，双击“QuickIP服务器”图标。

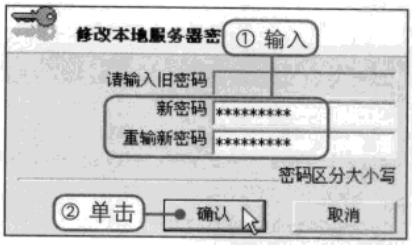
② 单击“确定”按钮

弹出“QuickIP服务器”提示框，提示用户设置密码，单击“确定”按钮。



③设置本地服务器密码

弹出“修改本地服务器密码”对话框，①在下方的文本框中输入设置的密码。②单击“确定”按钮。

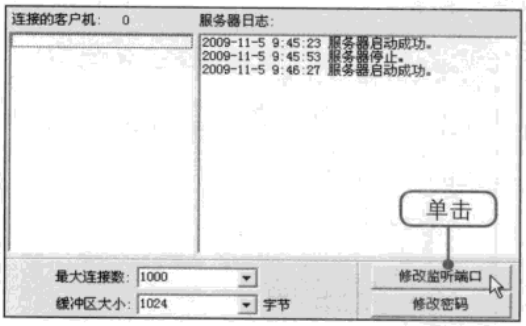


④删除用户

弹出“QuickIP服务器”提示框，提示用户密码修改成功，单击“确定”按钮。

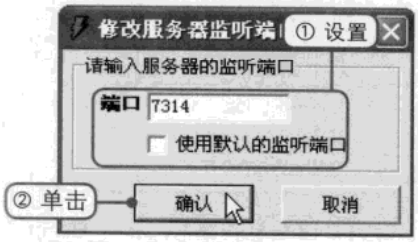
⑤打开“修改服务器监听端口”对话框

再次启动QuickIP服务器应用程序，在主界面中可以看见所有操作信息，接着单击“修改监听端口”按钮。



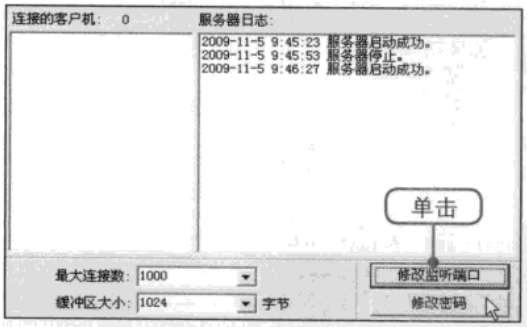
⑥修改服务器监听端口

打开“修改服务器监听端口”对话框，①取消勾选“使用默认的监听端口”复选框并在文本框中输入设置的端口。②单击“确认”按钮。



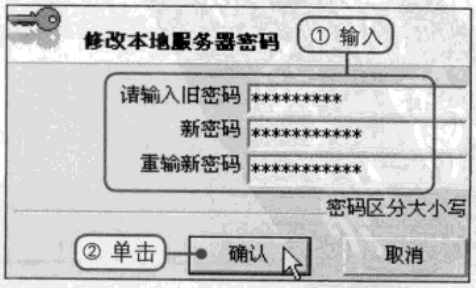
⑦打开“修改本地服务器的密码”对话框

返回主界面窗口，单击“修改监听端口”按钮，打开“修改本地服务器密码”对话框。



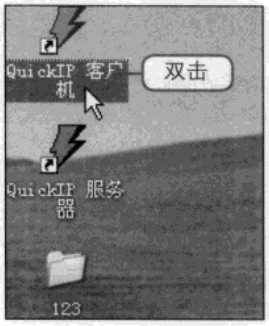
⑧修改本地服务器密码

①在文本框中分别输入旧密码和新密码。②单击“确认”按钮保存退出。



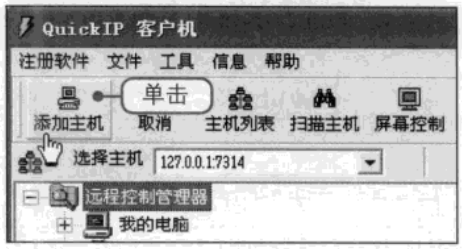
⑨ 启动QuickIP客户机

在桌面上双击“QuickIP客户机”快捷图标，启动QuickIP客户机应用程序。



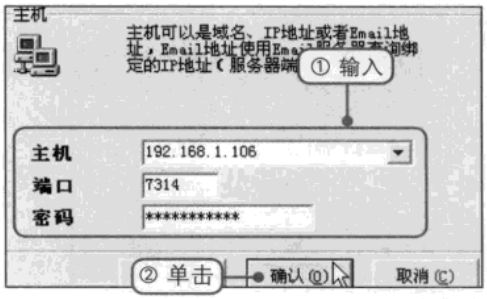
⑩ 打开“添加远程主机”对话框

打开“QuickIP客户机”主界面窗口，在窗口的工具栏中单击“添加主机”按钮，打开“添加远程主机”对话框。



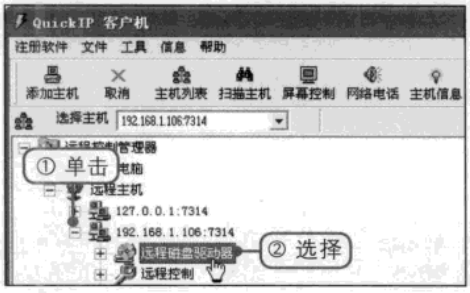
⑪ 添加远程主机

①在“主机”、“端口”、“密码”文本框中分别输入远程主机对应的信息。②单击“确认”按钮。



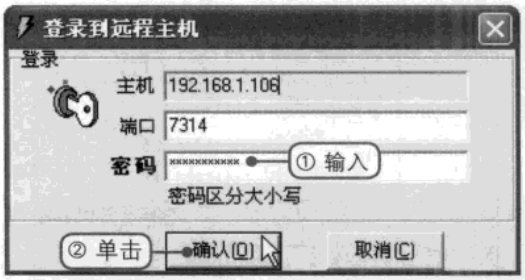
⑫ 查看远程磁盘驱动器

返回主界面窗口，①单击刚添加的远程主机IP地址前的展开按钮。②选择“远程磁盘驱动器”选项。



⑬ 登录远程主机

打开“登录到远程主机”对话框，①在“密码”文本框中输入正确的密码。②单击“确认”按钮。

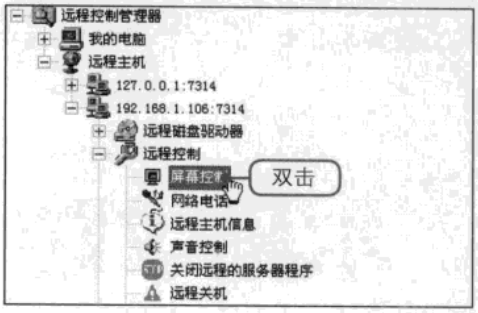


⑭ 查看远程磁盘驱动器

登录成功后返回主界面窗口，此时可以在“远程磁盘驱动器”子选项中看见所有的盘符，用户可对这些磁盘进行任何操作。

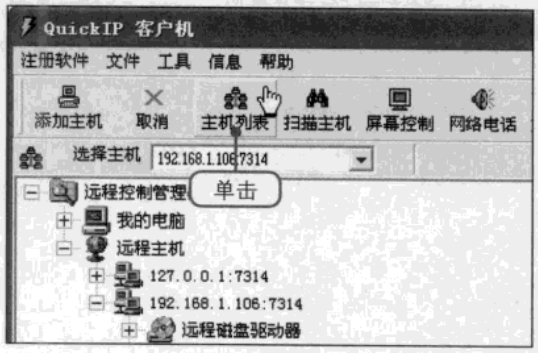
⑮ 查看屏幕控制

单击“远程控制”选项前的展开按钮，然后选择不同的选项。例如双击“屏幕控制”选项即可实现远程屏幕控制操作。



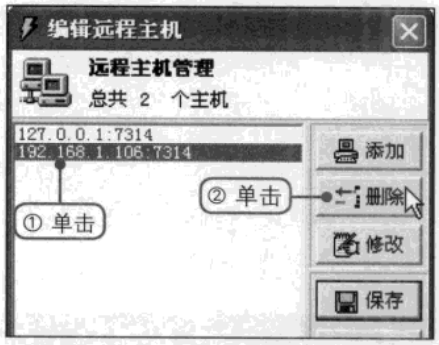
⑯ 打开“编辑远程主机”对话框

在窗口的工具栏中单击“主机列表”按钮，打开“编辑远程主机”对话框。



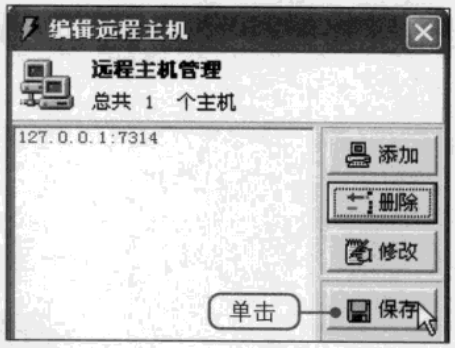
⑰ 删除远程主机

①在列表框中单击选中需要删除的远程主机。②在对话框的右侧单击“删除”按钮。

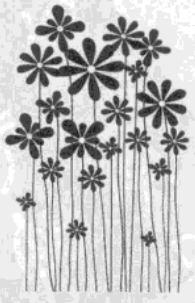


⑱ 保存退出

用户可以在列表框中看见远程主机已经被删除，直接单击“保存”按钮退出远程控制即可。



读书笔记



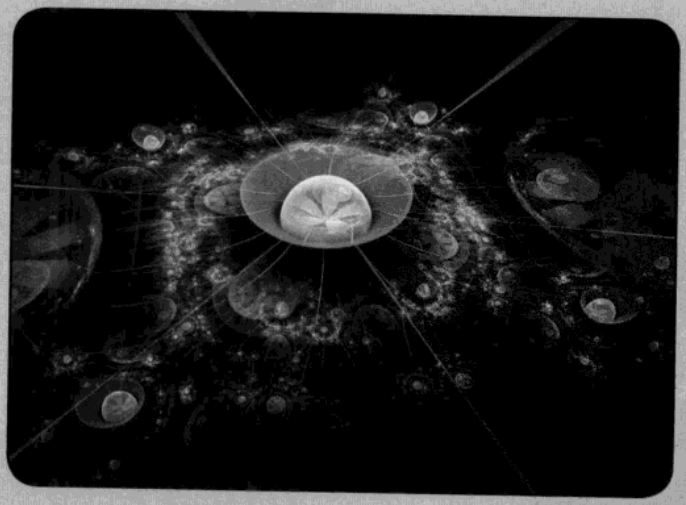
Chapter 13

木马攻防

重点知识

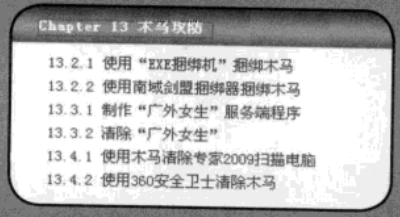
1. 木马基础知识
2. 捆绑木马
3. 黑客常用的木马工具——“广外女生”木马
4. 清除和阻止木马入侵电脑

在计算机领域中，木马是一类恶意程序，其主要目的是控制电脑，从而窃取目标电脑中的重要资料和密码。木马通常是捆绑在合法的程序之中，如使用“EXE捆绑机”、网页木马生成器等均可通过非常隐蔽的手段将木马与合法的程序绑定，当用户下载或使用该合法程序时，电脑就遭受了木马的入侵。因此用户需要随时防范木马，一旦木马入侵，必须及时对木马进行清除。



视频文件

参见随书光盘：视频教程\Chapter 13



13.1 木马基础知识

在互联网中，黑客们套用了古希腊人使用的特洛伊木马的思路，将木马植入合法的应用程序之中，并将这些带有木马的应用程序放入互联网中，当用户下载并使用这些应用软件时，木马就悄悄地进入用户的电脑，黑客入侵成功。

13.1.1 什么是木马

木马与前面介绍的病毒一样，也是一类电脑恶意程序。但是木马和病毒有着不同的地方，木马是被用来盗取其他用户的个人信息或者诱导目标用户执行该程序以达到盗取密码等各种数据资料等目的。

一个完整的木马系统由硬件、软件和具体连接三部分组成。

1 硬件部分

硬件部分是建立木马连接所必须的硬件实体。硬件实体包括控制端、服务端和Internet三部分，控制端是对服务端进行远程控制的一方， 服务端是被控制端远程控制的一方， 而Internet是控制端对服务端进行远程控制、数据传输的网络载体。

2 软件部分

软件部分是实现远程控制所必须的软件程序。软件程序包括控制端程序、木马程序和木马配置程序三部分。控制端程序是控制端用以远程控制服务端的程序，木马程序是潜入服务端内部，获取其操作权限的程序，木马配置程序是设置木马程序的端口号、触发条件、木马名称等，使其在服务端隐藏得更隐蔽的程序。

3 具体连接部分

具体连接部分是通过Internet在服务端和控制端之间建立一条木马通道所必须的元素。具体连接部分包括控制端IP/服务端IP和控制端端口/木马端口两部分。控制端IP/服务端IP，即控制端、服务端的网络地址，也是木马进行数据传输的目的地。控制端端口/木马端口，即控制端、服务端的数据入口，通过这个入口，数据可直达控制端程序或木马程序。

13.1.2 木马的特点

木马由于具有隐蔽性和欺骗性等特点，因此会长期潜伏在用户的电脑中不被轻易发现。

- 隐蔽性：木马是病毒的一种，它必须隐藏在用户的系统中并想尽一切办法不被发现，木马的隐蔽性主要体现在两个方面，一是它不会在桌面上产生任何图标，二是木马程序会自动在任务管理器中隐藏，并以“系统服务”的方式欺骗操作系统。
- 自动运行性：当用户启动系统时，木马程序必须随着启动运行而自动运行才能达到控制目标电脑的目的，因此木马必须潜伏在电脑中的启动配置文件中，例如win.ini, system.ini, winstart.bat以及启动组等文件中。
- 欺骗性：木马程序要达到其隐蔽的目的就必须借助系统中已有的文件，以防止被用户发

现。它一般都使用常见的文件名或扩展名，或者仿制一些不易被用户区分的文件名，甚至干脆借用系统文件中已有的文件名，只不过它保存在不同的路径之中。

13.1.3 木马的分类

随着时间的推移，木马的种类已经出现了很多，大多数的木马都不是单一类型的木马，往往具有很多种功能，可能还有一些至今没有发现的木马存在。尽管如此，大致可将木马分为破坏型、密码发送型、记录键盘型和查杀程序型木马。

- 破坏型：这种木马能够自动删除电脑上的某些重要文件，例如一些后缀名为 dll、ini、exe 的文件。
- 密码发送型：这种木马主要被用来盗窃用户的隐私信息，它能够把隐藏的密码找出来并且发送到指定的信箱，也可以用来盗窃用户的敏感口令等。
- 记录键盘木马：这种木马只做一件事情，就是记录中木马者的键盘敲击记录并且在硬盘的文件里查找密码，给木马使用者发送到指定的信箱。
- 查杀程序木马：这种木马主要用来关闭中木马者机器上运行的一些监控程序，让其他的木马更好地发挥作用。

13.2 捆绑木马

捆绑木马就是将木马程序和其他正常的程序捆绑在一起，当携带有木马的正常程序进入目标电脑时，木马也就成功地植入目标电脑并且不轻易被用户发现，起到了很好的伪装效果。

13.2.1 使用“EXE捆绑机”捆绑木马

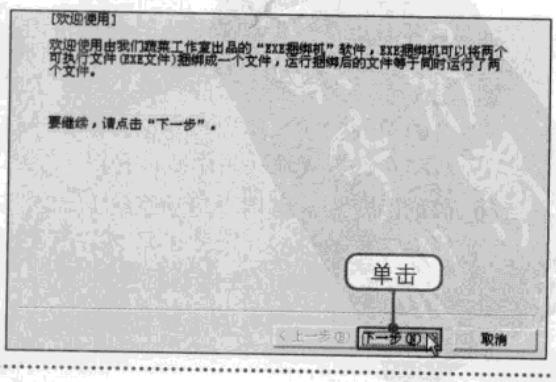
“EXE捆绑机”可以将两个后缀名为EXE的文件捆绑在一起，并且捆绑之后生成的文件图标与捆绑前的文件图标一模一样。

① 启动EXE捆绑机应用程序

由于该程序一般都比较小，直接将其解压到所在的文件夹窗口，然后双击对应的快捷图标即可启动程序。

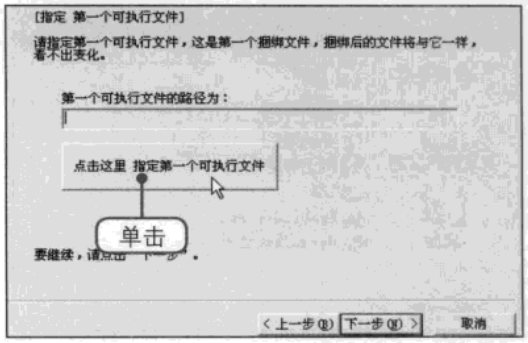
② 使用EXE捆绑机

打开“EXE捆绑机”对话框，直接单击“下一步”按钮。



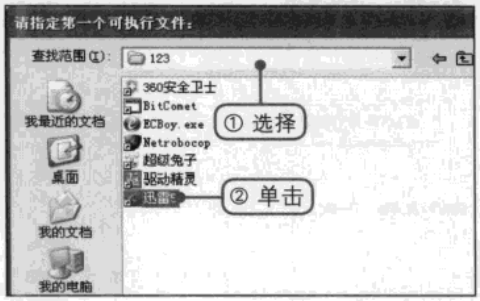
③ 打开路径选择对话框

切换至新的界面，单击“点击这里，指定第一个可执行文件”按钮。



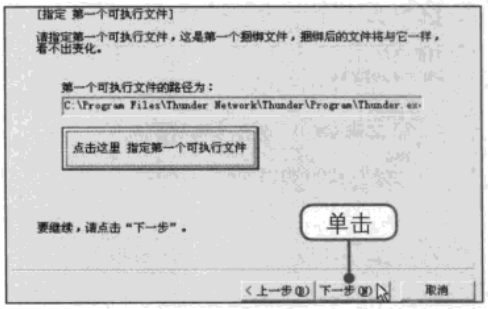
④ 选择第一个可执行文件

打开“请指定第一个可执行文件”对话框，①在“查找范围”下拉列表中选择文件所在的路径。②在列表框中单击以选中可执行文件。



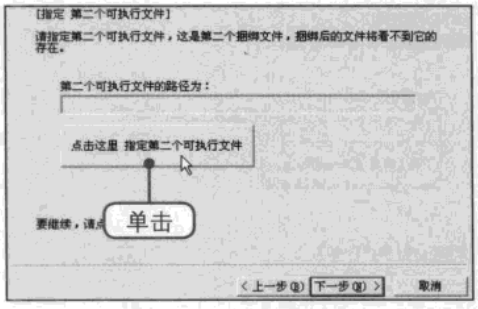
⑤ 确认选择的路径

单击“打开”按钮返回上一级对话框，确认选择的路径无误后单击“下一步”按钮。



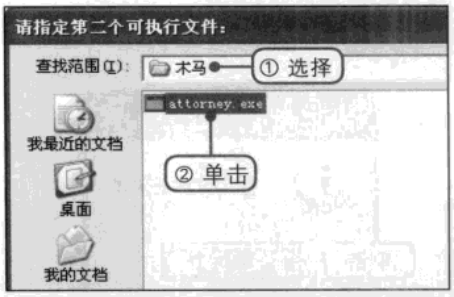
⑥ 打开路径选择对话框

在打开的对话框中单击“点击这里 指定第二个可执行文件”按钮。



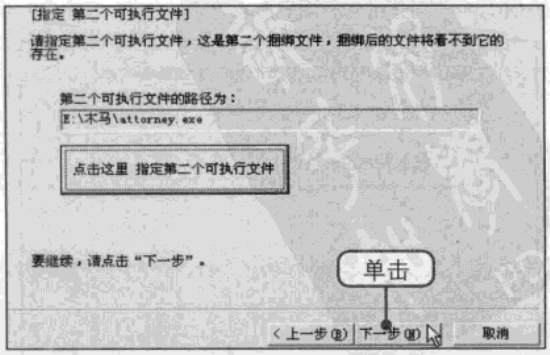
⑦ 选择第二个可执行文件

打开“请指定第二个可执行文件”对话框，①在“查找范围”下拉列表中选择文件所在的位置。②在列表框中单击以选中文件。



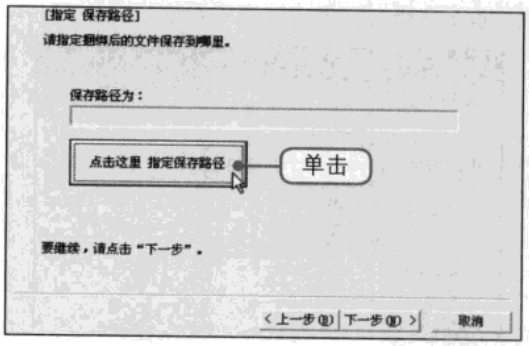
⑧ 确认选择的路径

单击“打开”按钮返回上一级对话框，确认选择的路径无误后单击“下一步”按钮。



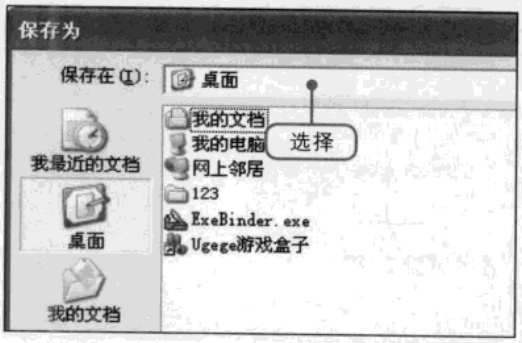
⑨ 打开“保存为”对话框

切换至新的对话框，单击“点击这里，指定保存路径”按钮，打开“保存为”对话框。



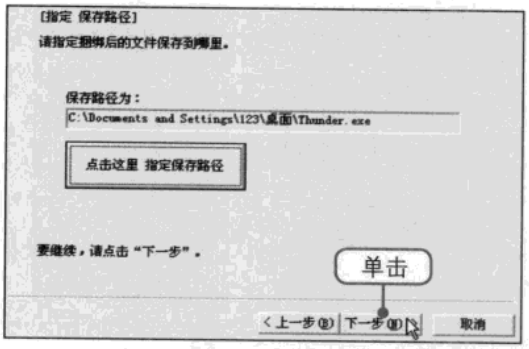
⑩ 设置保存路径

在“保存在”下拉列表中选择文件保存的位置。选中后单击“打开”按钮返回上一级对话框。



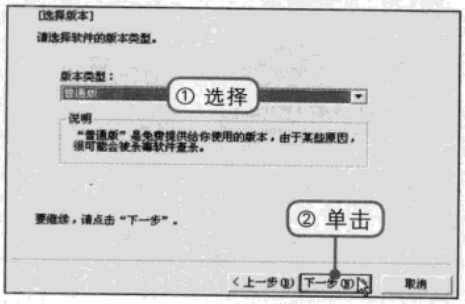
⑪ 确认保存路径

在对话框中确认设置的保存路径是否正确，确认无误后直接单击“下一步”按钮。



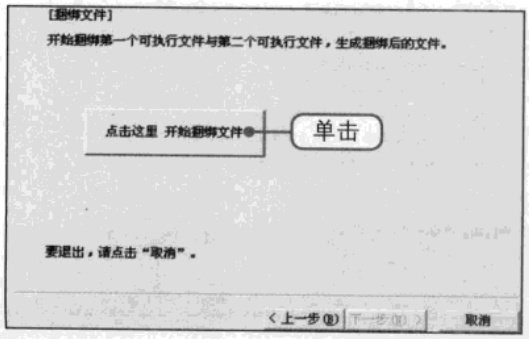
⑫ 选择版本类型

切换至新的对话框，①在“版本类型”下拉列表中选择版本类型，例如选择“普通版”。②单击“下一步”按钮。



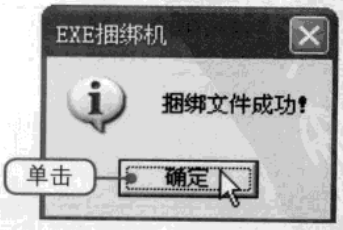
⑬ 开始捆绑文件

切换至新的对话框，单击“点击这里 开始捆绑文件”按钮开始捆绑文件。



⑭ 捆绑成功

捆绑完成后弹出“EXE捆绑机”对话框，提示用户捆绑成功，单击“确定”按钮。

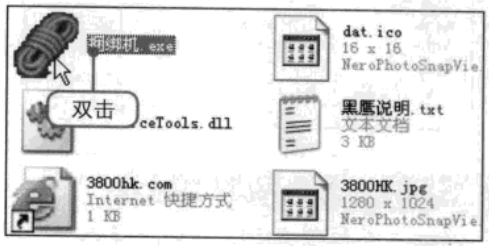


13.2.2 使用南域剑盟捆绑器捆绑木马

“南域剑盟捆绑器”不但具有最基本的捆绑功能，而且还可以设置在运行后将文件释放到指定的区域，还可以设置捆绑后生成文件的属性，以及设置该文件更具隐蔽性和破坏性。

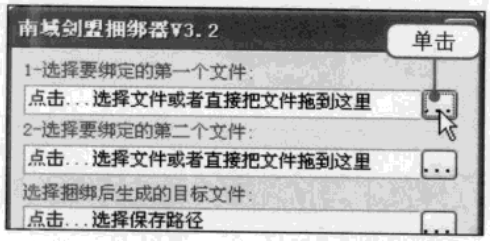
① 启动南域剑盟捆绑器

由于该捆绑器比较小，解压到所在的文件夹后双击快捷图标即可启动南域剑盟捆绑器。



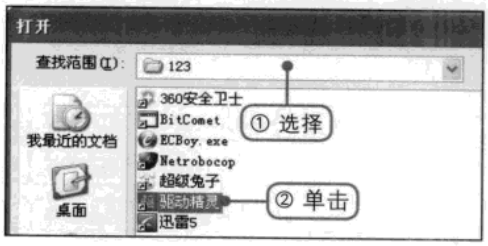
② 设置要捆绑的第一个文件

打开其主界面窗口，单击“选择要绑定的第一个文件”选项下的...按钮。



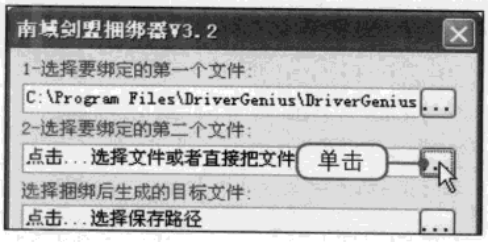
③ 选择要绑定的第一个文件

打开“打开”对话框，①在“查找范围”下拉列表中选择第一个文件所在的路径。②在列表框中单击以选中要绑定的文件。



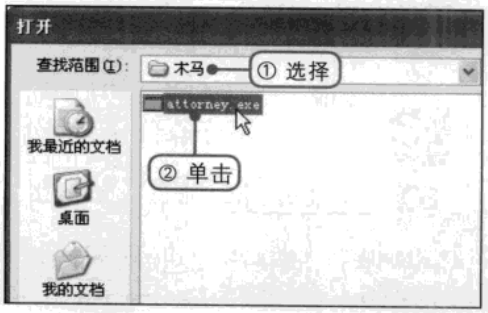
④ 设置要捆绑的第二个文件

单击“打开”按钮返回主界面窗口，接着在窗口中单击“选择要绑定的第二个文件”选项下的...按钮。



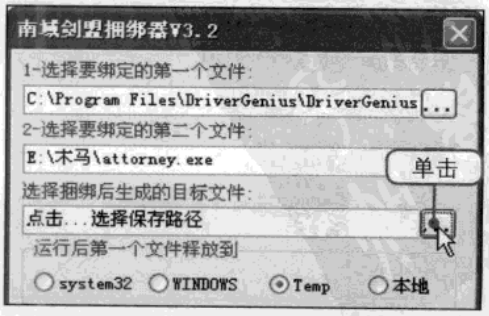
⑤ 选择要绑定的第二个文件

弹出“打开”对话框，①在“查找范围”下拉类表中选择木马文件所在的路径。②在列表框中单击木马文件。



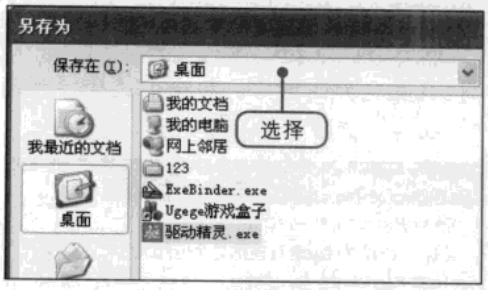
⑥ 设置保存路径

单击“打开”按钮返回主界面窗口，在“选择捆绑后生成的目标文件”选项卡下单击...按钮。



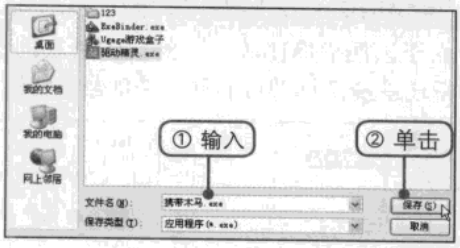
⑦ 选择保存路径

打开“另存为”对话框，在“保存在”下拉列表中选择保存捆绑文件的路径，例如选择桌面。



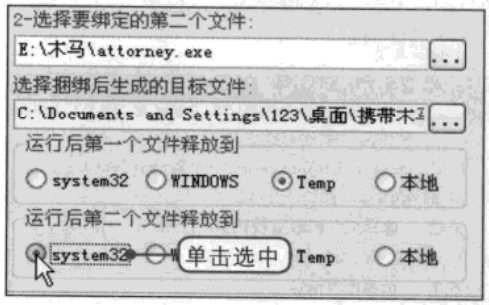
⑧ 设置捆绑文件的名称

①在“另存为”对话框下方的“文件名”文本框中输入捆绑文件的名称，例如输入“携带木马”。②单击“保存”按钮。



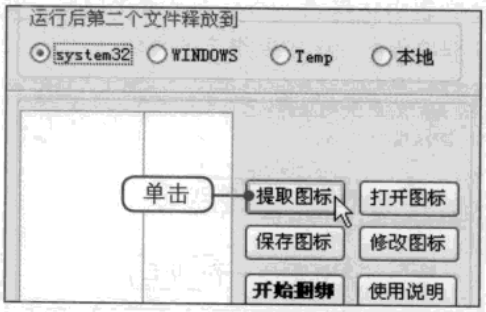
⑨ 选择木马文件运行后的释放位置

返回主界面窗口，将“运行后第一个文件释放到”选项组的设置保持默认，然后单击选中“运行后第二个文件释放到”选项组中的system32单选按钮。



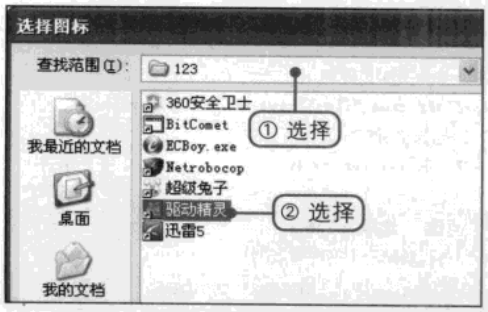
⑩ 单击“提取图标”按钮

设置完毕后在窗口的中间区域单击“提取图标”按钮。



⑪ 选择图标

打开“选择图标”对话框，①在“查找范围”下拉列表中选择路径。②在列表框中选择图标。建议选择第一个文件的图标。



⑫ 设置捆绑文件的属性

单击“打开”按钮返回主界面窗口，①在窗口中选中图标后在下方设置捆绑文件的属性，②单击选中“隐藏属性”单选按钮。

⑬ 修改捆绑文件的时间

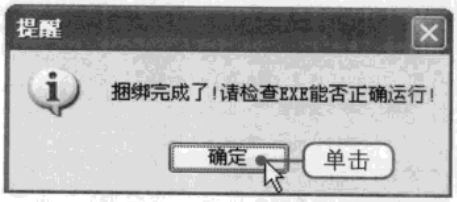
①在对话框的底部修改捆绑文件的创建、修改时间，如下图所示。②修改完毕后单击“修改文件时间”按钮。

⑭ 开始捆绑

设置完毕后在对话框的中部单击“开始捆绑”按钮。

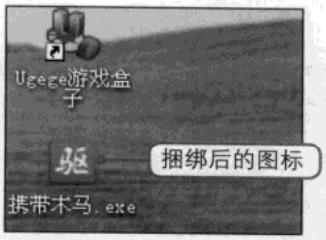
⑮ 捆绑完成

捆绑完成后弹出“提醒”对话框，提示用户捆绑完成，请检查EXE能够正确运行，直接单击“确定”按钮。



⑯ 查看捆绑后的图标

打开前面设置的保存路径，这里返回到桌面，此时可在桌面上看见捆绑后的图标。



13.3 黑客常用的木马工具——“广外女生”木马

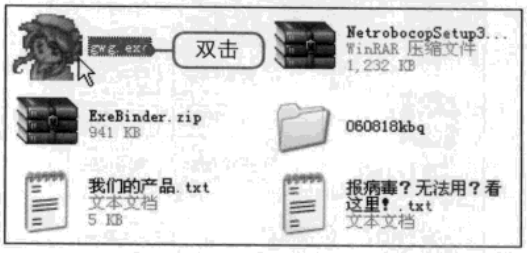
“广外女生”木马是一个可以运行在Windows的各个版本中的远程控制软件，虽然该木马采用的技术和其控制功能并不是那么的高明和强悍，但是由于该木马具有超高的“免疫”能力，就算用户的电脑中安装了杀毒软件和防火墙也很难避免，该木马除了具有普通木马的功能以外，还具有服务端程序体积小，注册表编辑器及任务管理器界面直观，易于操作等特点。该木马之所以流行在于它具有关闭网络安全防护软件的功能。

13.3.1 制作“广外女生”服务端程序

制作木马程序其实就是制作服务端程序，制作完成后就可将其植入目标电脑，然后便可实现远程控制。

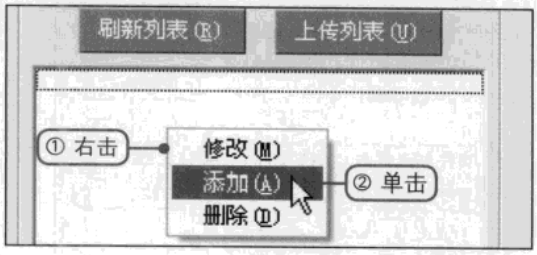
① 启动“广外女生”应用程序

由于该应用程序比较小，用户下载并解压到电脑中以后，双击其快捷图标即可启动该应用程序。



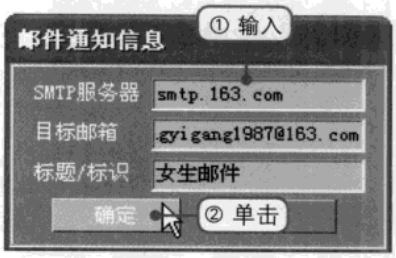
② 添加邮箱信息

①切换至“服务端设置”选项卡下，接着在“对方邮件通知列表”列表框空白处右击，②在弹出的快捷菜单中单击“添加”命令。



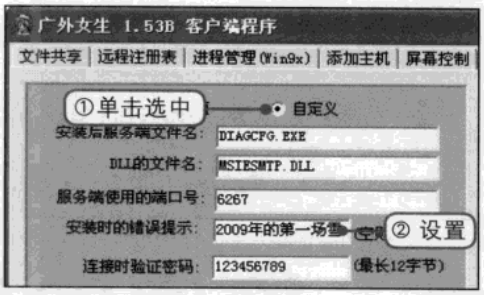
③ 设置邮件通知信息

弹出“邮件通知信息”对话框，①在对话框中的3个文本框中输入对应的信息。②单击“确定”按钮。



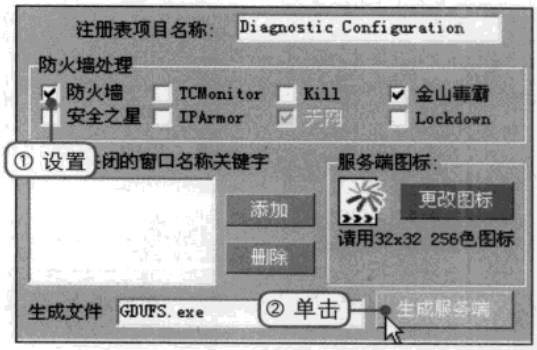
④ 设置服务端的相关信息

①在对话框中左侧单击选中“自定义”单选按钮。②在下方设置相关的选项，例如设置安装时的错误提示。



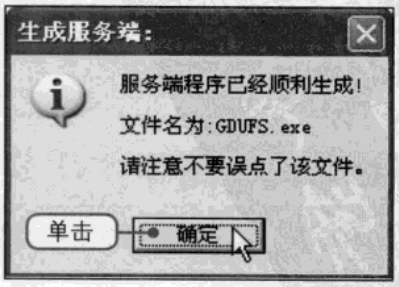
⑤ 设置其他选项

①在“防火墙处理”选项组中勾选“防火墙”复选框。②单击“生成服务端”按钮。



⑥ 生成服务端

弹出“生成服务端”对话框，提示用户服务端程序已经顺利生成，直接单击“确定”按钮。



13.3.2 清除“广外女生”

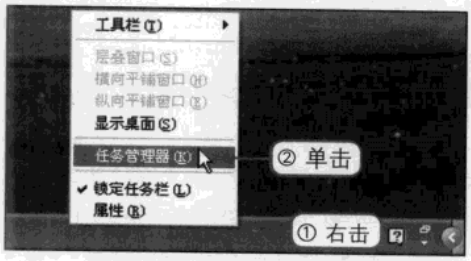
从前面配置的服务端程序可知道该木马运行的是6267号端口，因此可使用netstat –a来查看电脑是否开放了6267号端口，若开放了此端口，该电脑就很可能已经中毒了。用户可通过前面设置的详细信息手动将其删除。

① 查看开放的端口

打开“命令提示符”窗口，输入netstat –a后按Enter键即可查看6267号端口是否开启。

② 打开任务管理器

①右击任务栏空白处。②在弹出的快捷菜单中单击“任务管理器”命令，打开“Windows任务管理器”窗口。

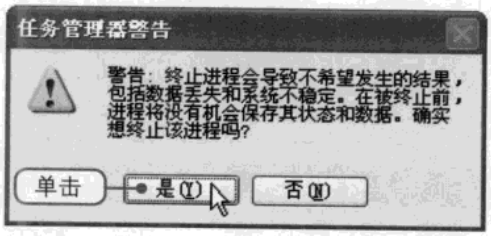


③ 结束木马对应的进程

切换至“进程”选项卡，①右击DIAGCFG.EXE选项。②在弹出的快捷菜单中单击“结束进程”命令。

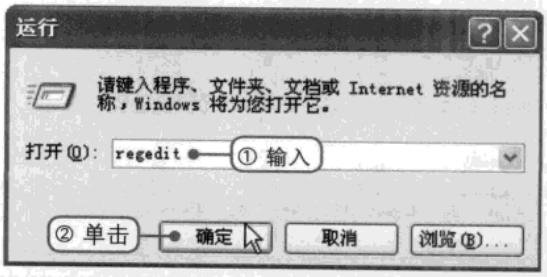
④ 确认结束

弹出“任务管理器警告”对话框，直接单击“是”按钮结束该进程。



⑤ 打开注册表编辑器

打开“运行”对话框，①在文本框中输入regedit命令。②单击“确定”按钮。



⑥ 查找command子键

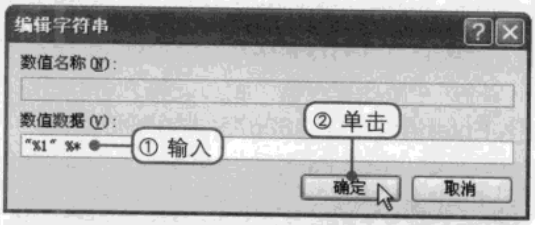
在打开的“注册表编辑器”窗口的左侧单击HKEY_LOCAL_MACHINE\SOFTWARE\classes\exefile\shell\open\command子键。

⑦ 打开“编辑字符串”对话框

①右击窗口右侧的“默认”键值项。②在弹出的快捷菜单中单击“修改”命令。

⑧ 编辑字符串

弹出“编辑字符串”对话框，①在“数值数据”文本框中将数据修改为“%1” %*”。②单击“确定”按钮退出。

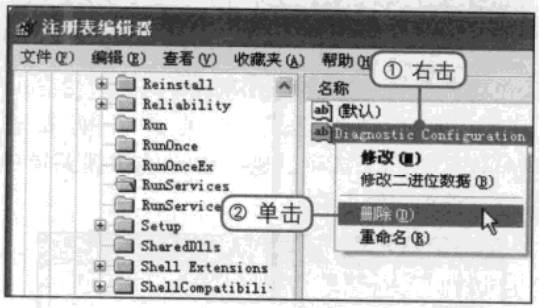


⑨ 查找RunServices子键

在“注册表编辑器”窗口左侧单击HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices子键。

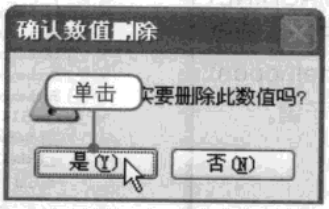
⑩ 删除目标键值项

①在窗口右侧右击Diagnostic Configuration选项。②在弹出的快捷菜单中单击“删除”命令。



⑪ 确认删除该数值

弹出“确认数值删除”对话框，直接单击“是”按钮确认删除该数值。



⑫ 删除木马文件

进入C:\Windows\system32目录下，①右击DIAGCGFG.EXE文件。②在弹出的快捷菜单中单击“删除”命令即可删除木马文件。

13.4 清除和阻止木马入侵电脑

清除木马可以自己动手进行，也可以使用专业的软件进行清除。用户若要手动清除木马，则需要确定木马的程序、入侵端口、隐藏位置和清除的方式，这种清除方式对于刚刚接触计算机的人是有很大困难的，因此用户可使用一些专业查杀木马的软件来扫描并清理计算机中的木马，并让这些软件对计算机进行实时监控。

13.4.1 使用木马清除专家2009扫描电脑

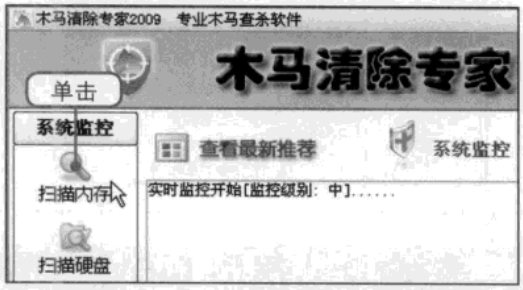
木马清除专家是一款专业查杀木马的软件，该软件除了采用传统病毒库查杀木马之外，还能智能查杀未知变种木马，自动监控内存可疑程序并且实时查杀内存硬盘木马。木马清除专家采用了第二代木马扫描内核，查杀木马快速。该软件还具有内存优化功能、网络入侵拦截、IE修复、恶意网站拦截系统修复、系统进程管理和启动项目管理等功能。

① 启动木马清除专家

用户下载并安装该软件之后会在桌面上出现对应的快捷图标。双击该图标启动木马清除专家2009。

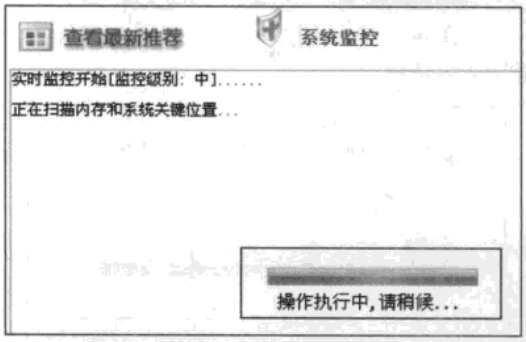
② 扫描内存

打开软件的主界面窗口，在窗口的左侧单击“扫描内存”选项。



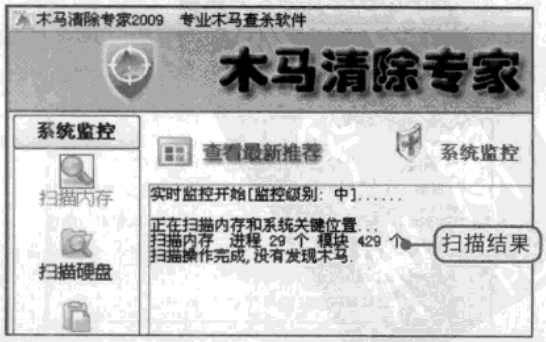
③ 扫描内存和系统关键位置

此时可在窗口的右侧看见该软件开启实时监控并正在扫描内存和系统关键位置，请耐心等待。



④ 查看扫描结果

扫描完毕后在窗口右侧会显示扫描的结果，若扫描到木马，则用户可直接将其清除。

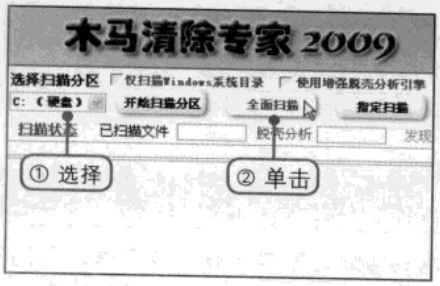


⑤ 扫描硬盘

在主界面窗口的左侧单击“扫描硬盘”选项进行硬盘扫描。

⑥ 全面扫描

①在窗口右侧选择扫描分区，例如选择C盘。②单击右侧的“全面扫描”按钮。



⑦ 查看扫描的进度

开始扫描选中的C盘，此时可在窗口右侧看见扫描的进度，请耐心等待。

⑧ 扫描结束

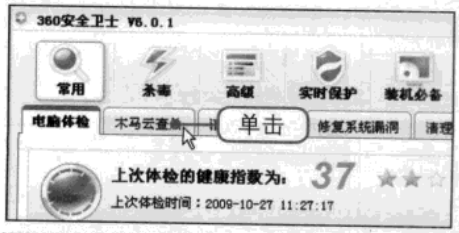
扫描结束后可在窗口右侧看见扫描的结果，若有木马则可直接将其清除。

13.4.2 使用360安全卫士清除木马

使用360安全卫士不仅可以扫描并清除电脑中存在的木马，还可以开启实时监控以防止木马入侵电脑。

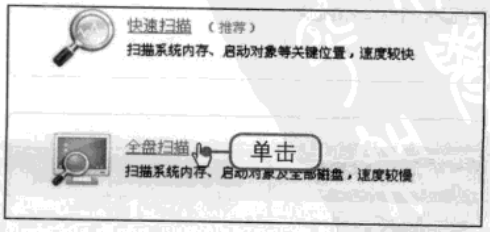
① 木马云查杀

打开360安全卫士主界面，单击“木马云查杀”标签，打开“360木马云查杀”选项卡。



② 全盘扫描

选择查杀木马的方式，例如单击“全盘扫描”文字链接。

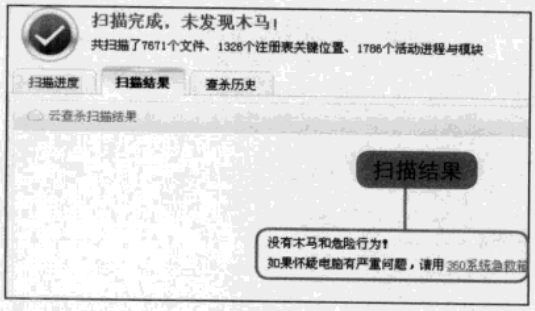


③ 查看扫描的进度及详细信息

此时开始对电脑进行全面扫描，用户可在窗口中看见扫描的进度以及扫描的类型，请耐心等待。

④ 扫描完毕

扫描完毕后窗口自动跳转至扫描结果界面，若发现木马则可单击下方的“立即清理”按钮清除木马，若没有发现木马则直接单击“返回”按钮即可。



360安全卫士查杀木马的三种方式

360安全卫士查杀木马有快速扫描、全面扫描和自定义扫描三种方式。

- 快速扫描：扫描的范围包括初始化扫描环境、开机启动项、系统敏感启动项等，快速扫描不扫描磁盘，主要扫描系统内存、启动对象等关键位置，扫描速度较快。
- 全盘扫描：扫描的范围不仅包括初始化扫描环境、开机启动项和系统敏感启动项等，而且对电脑的所有磁盘进行详细的扫描，使用全盘扫描的速度较慢。
- 自定义扫描：自定义扫描与全面扫描的主要区别在于用户需要选择扫描的磁盘范围，而全盘扫描是指扫描电脑中的所有磁盘分区。用户若使用自定义扫描，则可选择电脑中的某一分区或者某几个分区进行扫描。

读书笔记

Chapter 14

QQ攻防

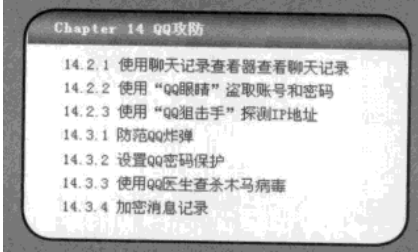
重点知识

1. 黑客攻击QQ的常用方式
2. 攻击QQ的各种手段
3. 保护QQ的各种手段

QQ软件由于其功能强大成为目前国内使用最为广泛的聊天工具之一。一些用户常常将比较重要的文件或者数据放在QQ网络硬盘中，还有一些用户喜欢在QQ中充入大量的Q币玩游戏或买QQ秀，这就使QQ成为了有利可图的入侵对象，于是便发生了QQ被盗的事件。用户若想防止QQ被盗，除了需要了解黑客常用的攻击手段之外，还需要做好保护QQ的安全措施及登录QQ的环境安全。

视频文件

参见随书光盘：视频教程\Chapter 14



14.1 黑客攻击QQ的常用方式

在使用QQ时，常常会有陌生人请求用户将其加为好友，一旦将黑客加为好友，他就会使用各种手段来破坏用户的QQ或者盗取用户QQ的密码。例如使用炸弹攻击导致电脑死机，或者使用暴力破解、木马程序等手段盗取用户QQ的密码。

1 使用炸弹进行攻击

黑客使用炸弹对用户的QQ进行攻击大部分是恶作剧，例如将一个图片文件放入一个空文件夹中，然后不断地复制粘贴，当该文件夹中拥有成百上千的图片时，全部选中这些图片并使用QQ同时发送给一个用户，对方就会一直接收文件，这样很有可能造成对方QQ掉线或者死机。

2 使用QQ木马和病毒

QQ木马和病毒主要通过网页传播、伪装成QQ进行传播和与QQ安装软件捆绑在一起进行传播三种方式，当QQ木马和病毒入侵电脑时就会造成QQ被迫下线、死机等情况，严重时还会破坏电脑。

3 盗取对方的QQ密码

黑客盗取对方QQ密码的手段包含暴力破解、专门的破解工具和使用木马程序等。

暴力破解是指使用密码词典中的密码一个接一个地对用户QQ的密码进行尝试，直到尝试出正确的密码，这种方法成功几率不高，耗费时间多，技术成分低，也称为穷举法。

专门的破解工具包含两种，一种是直接破解选中过“下次登录不显示登录框”的本地QQ号，但是只能破解该QQ号的最后一次登录密码。另一种是使用了一种叫做“隐身穿墙术”的QQ黑软，它通过使用一个独立的执行文件调用QQ主程序，跳过密码验证直接登录QQ。

黑客可通过诱骗用户去浏览携带有QQ木马的网页，一旦打开该网页，QQ木马就自动下载并运行。黑客还可通过向用户QQ发送捆绑了木马的软件、图片等文件让其执行，木马通过获取QQ登录窗口的密码或者记录键盘的操作来盗取密码。

14.2 攻击QQ的手段

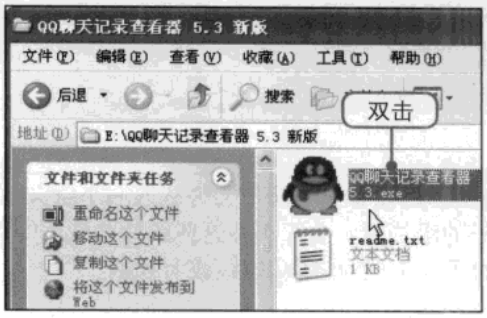
如今的电脑里几乎都安装了QQ软件，许多人也几乎都有自己的QQ号，而使用的人多了，有关QQ安全的问题也就多了。本节介绍攻击QQ的一些手段，使读者能够及时采取相应的预防措施。

14.2.1 使用聊天记录查看器查看聊天记录

聊天记录查看器是一款查看本地电脑聊天记录的软件，使用该软件可有效监控及查阅本机登录过的QQ聊天记录。

① 启动聊天记录查看器

下载后将文件解压至本地电脑中，双击“聊天记录查看器”快捷图标。

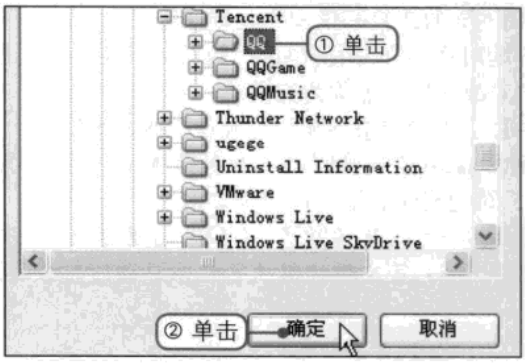


② 打开“浏览文件夹”对话框

打开“选择QQ目录和号码”对话框，直接单击“选择目录”按钮。

③ 选择QQ的安装目录

打开“浏览文件夹”对话框，①在列表框中单击QQ的安装目录。②单击“确定”按钮。

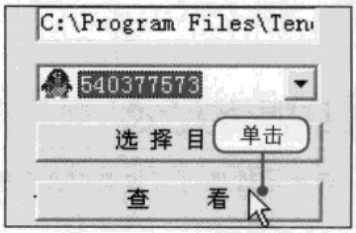


④ 选择QQ号码

返回“选择QQ目录和号码”对话框，①单击对话框中的下三角按钮。②在弹出的下拉列表中选择需要查看聊天记录的QQ号码。

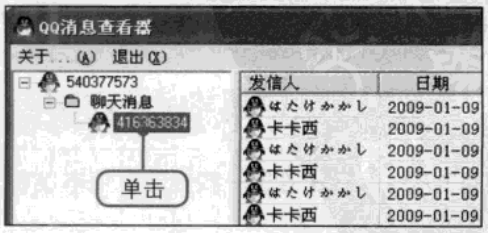
⑤ 打开“QQ消息查看器”窗口

选中后直接单击下方的“查看”按钮开始查看该QQ号码的聊天记录，打开“QQ消息查看器”窗口。



⑥ 查看聊天记录

在窗口左侧单击“聊天消息”选项前的展开按钮，接着单击选中该QQ的聊天对象，此时可在窗口右侧看见其详细的聊天记录。

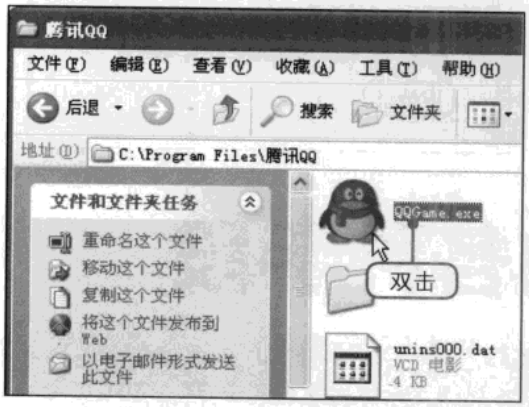


14.2.2 使用“QQ眼睛”盗取账号和密码

“QQ眼睛”是一种常用的盗号木马，当“QQ眼睛”被放置在用户电脑中后，该工具便会记录下用户的QQ号码及其密码并将其发送至指定的邮箱中。

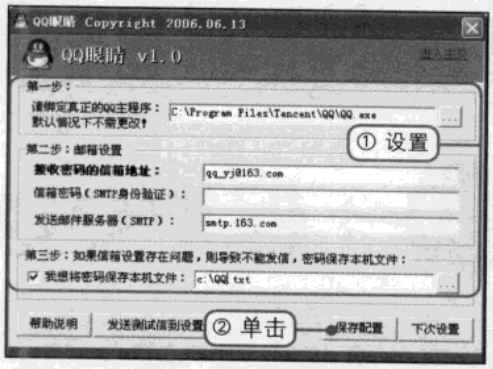
① 启动QQ眼睛

用户下载并将其解压至本地电脑中，双击窗口中对应的快捷图标，启动QQ眼睛应用程序。



② 打开“浏览文件夹”对话框

打开“QQ眼睛”主界面窗口，①在主界面中设置QQ.exe的路径、接收密码的电子邮箱地址、密码，以及当信箱无法接收时将密码存储在本地电脑中。②设置完毕后单击“保存配置”按钮。



14.2.3 使用“QQ狙击手”探测IP地址

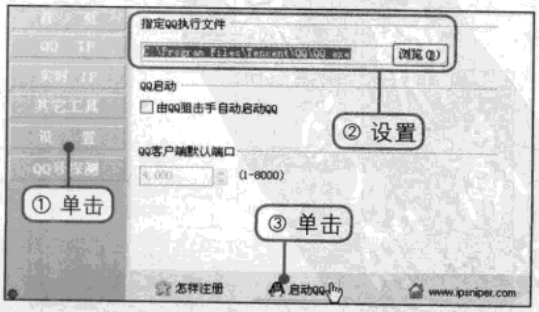
QQ狙击手是一款探测IP地址的软件，该软件能够探测QQ好友、腾讯服务器及腾讯广告服务器代理的IP地址及端口等。

① 启动QQ狙击手

下载并安装好QQ狙击手之后会在桌面上出现对应的快捷图标，双击该图标启动QQ狙击手应用程序。

② 设置QQ狙击手

打开“QQ狙击手”主界面窗口，①单击“设置”按钮。②在右侧设置“指定QQ执行文件”选项。③单击“启动QQ”按钮。

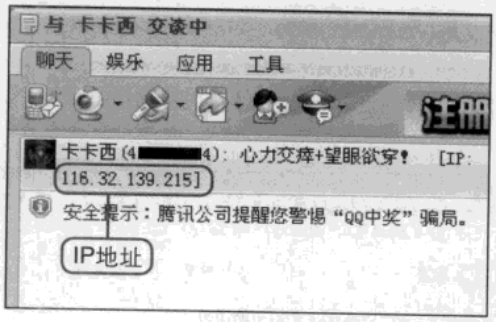


③ 登录QQ

打开QQ用户登录窗口，①在窗口中输入有效的QQ账号和密码。②单击“登录”按钮。

④ 查看好友的IP地址

登录成功后在QQ好友面板中双击好友的头像，打开对应的聊天窗口，此时可在窗口的顶部看见对方的IP地址。



14.3 保护QQ的各种手段

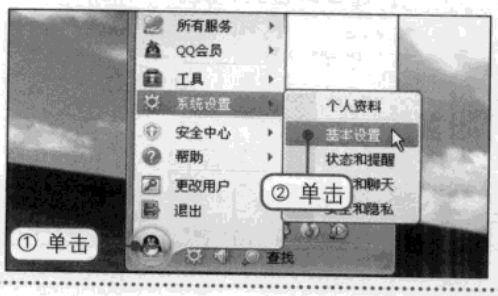
随着QQ功能的日益强大，越来越多的人使用QQ，当用户在申请QQ之后要立即填写密保资料，当QQ丢失后可使用密保资料找回并重新设置密码。除此之外，还需要防范QQ炸弹的攻击，并在电脑中安装QQ医生查杀QQ盗号木马和病毒，以确保QQ的安全使用。

14.3.1 防范QQ炸弹

QQ炸弹是指对方在短时间内发送大量的信息导致用户QQ掉线或者电脑死机，因此可通过拒绝陌生人的消息来防范QQ炸弹。如果是在其他人的电脑上登录QQ，则首先需要设置退出QQ时自动清除所有消息记录以防聊天记录泄露。

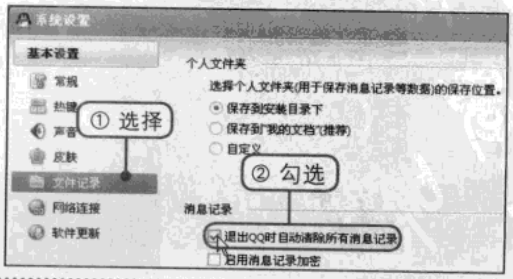
① 打开“系统设置”对话框

用户登录QQ后，①单击主界面上的“主菜单”按钮。②单击“系统设置>基本设置”命令，打开“系统设置”对话框。



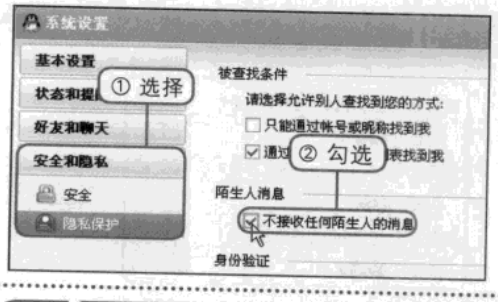
② 设置自动清除所有消息记录

①选择左侧的“文件记录”选项。②在“消息记录”选项组中勾选“退出QQ时自动清除所有消息记录”复选框。



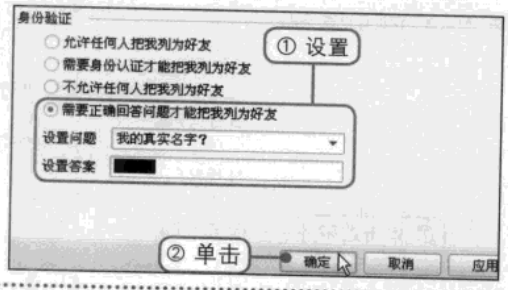
③ 设置不接收任何陌生人的消息

①选择“安全和隐私>隐私保护”选项。②在“陌生人消息”选项组中勾选“不接收任何陌生人的消息”复选框。



④ 设置身份验证

①单击选中“需要正确回答问题才能把我列为好友”单选按钮并设置问题和答案。②单击“确定”按钮保存退出。



QQ尾巴

“QQ尾巴”实际上是一种恶意病毒，中了该病毒的QQ会自动向用户的在线的好友发送正常的对话信息，其中包括“快去这看看，里面有好多的免费电影……”之类的假消息，一旦用户点击了这个网站，则网站上携带的病毒就会入侵电脑，电脑遭受该类病毒的入侵之后，用户的QQ就会向QQ中的好友一个个地传播这个携带有病毒的网站。

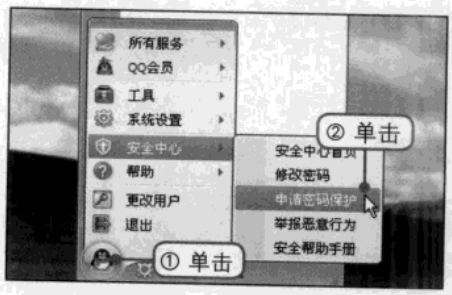
若要防范“QQ尾巴”就需要及时下载并安装系统、浏览器的升级补丁，并且不要轻易地点击聊天信息中的网站链接。

14.3.2 设置QQ密码保护

当成功申请一个QQ号码之后，系统会提示用户立即设置QQ密码保护，若果及时设置了QQ密码保护，而由于偶然原因QQ被人盗取时，则可直接使用QQ密码保护找回QQ号码并重新设置QQ密码。

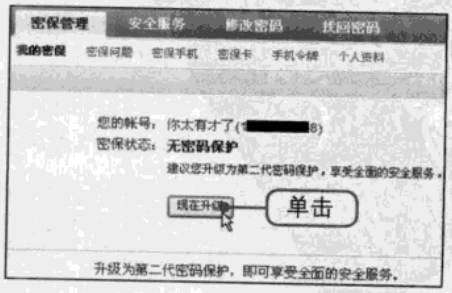
① 单击“申请密码保护”命令

登录QQ之后，①单击主界面中的“主菜单”按钮。②在弹出的菜单汇总单击“安全中心>申请密码保护”命令。



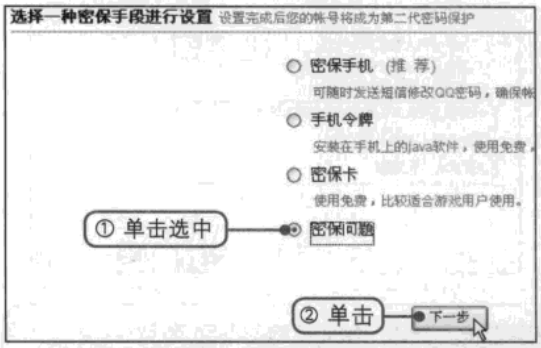
② 单击“现在升级”按钮

打开“QQ安全中心”页面，在“密保管理”选项卡中可以看见密保状态为无密码保护，单击“现在升级”按钮。



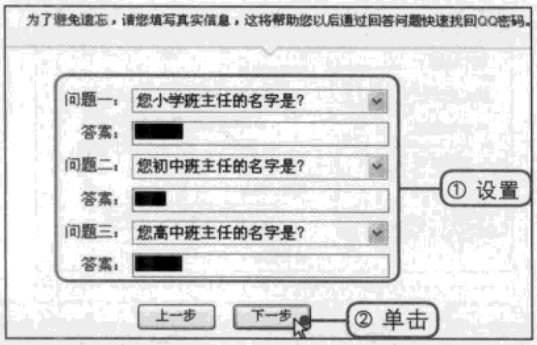
③ 单击选中“密保问题”单选按钮

打开新的页面，①在页面中选中一种密保手段进行设置，例如单击选中“密保问题”单选按钮。②单击“下一步”按钮。



④ 设置密保问题及答案

①在打开的界面中设置3个问题以及对应的答案，设置完毕后要牢牢记住。②单击“下一步”按钮。

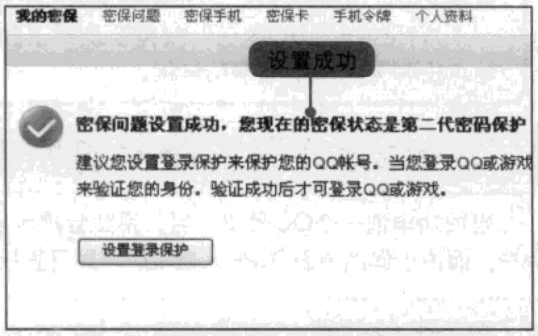


⑤ 再次输入密保问题的答案

①在打开的界面中再次输入密保问题对应的正确答案。②单击“下一步”按钮。

⑥ 设置成功

打开新的页面，显示“密保问题设置成功”等字样，即密保问题设置成功。



多种密保手段设置

在设置密码保护时可选择不同的密保手段对QQ进行保护，如密保手机、手机令牌、密保卡和密保问题。

使用密保手机就是将QQ号码与手机绑定，用户可随时通过发送短信修改QQ密码，即使QQ被盗，只需发条短信即可修改密码并重新登录。

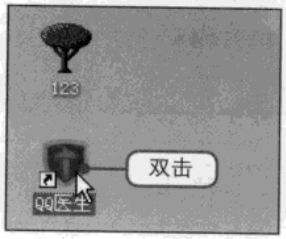
手机令牌是安装在手机上的java软件，用户可免费使用，若喜欢玩腾讯公司推出的游戏，可使用手机令牌有效地保障游戏用户账户安全。

14.3.3 使用QQ医生查杀木马病毒

“QQ医生”是腾讯公司针对盗取QQ密码的木马病毒专门开发的一款安全软件，它能够准确地扫描用户电脑上的盗号木马并有效清除。

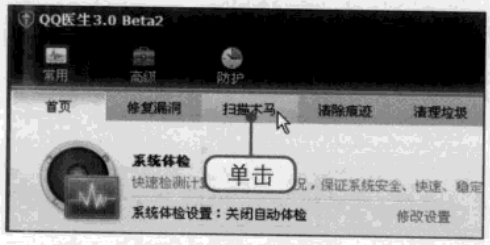
① 启动QQ医生

下载并安装好QQ医生后会在桌面上出现对应的快捷图标，双击该图标启动QQ医生应用程序。



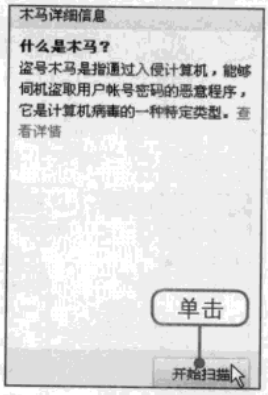
② 切换至“扫描木马”选项卡

打开QQ医生主界面窗口，单击“扫描木马”标签，切换至该选项卡。



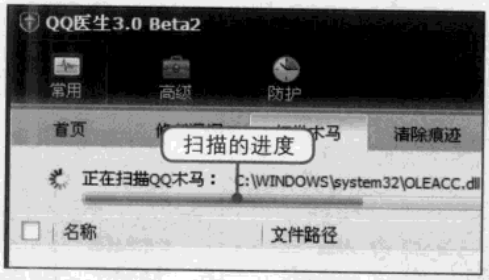
③ 开始扫描木马

在窗口的右下角单击“开始扫描”按钮开始扫描系统中的木马。



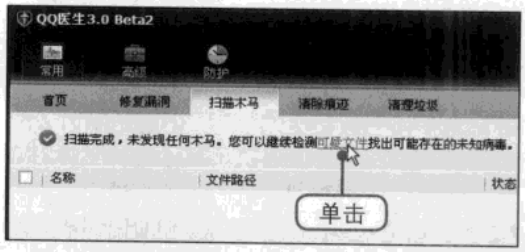
④ 查看扫描的进度

此时在窗口的顶部可以看见该软件扫描电脑中盗号木马的进度以及详细信息，只需耐心等待即可。



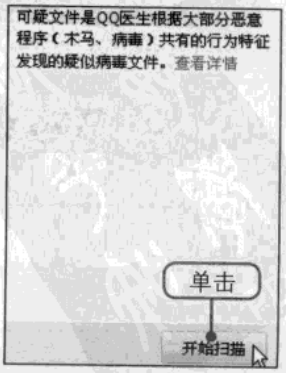
⑤ 单击“可疑文件”文字链接

扫描完成后，若发现木马则可手动进行清除，若未发现木马则单击“可疑文件”文字链接切换至该选项卡。



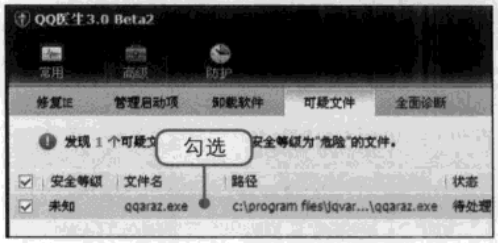
⑥ 开始扫描可疑文件

在窗口的右下角单击“开始扫描”按钮扫描电脑内的可疑文件。



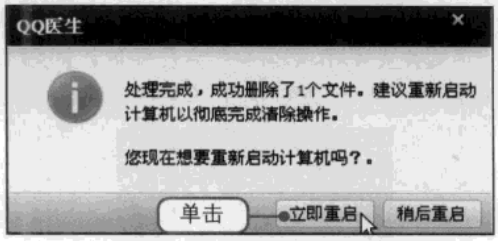
⑦ 删除可疑文件

扫描完成后若发现可疑文件，则会在窗口中显示出来可。勾选可疑文件复选框，接着单击“删除此文件”按钮即可删除可疑文件。



⑧ 重新启动电脑

弹出“QQ医生”提示框，提示用户重新启动电脑以彻底完成清除操作，单击“立即重启”按钮并重新启动电脑即可。

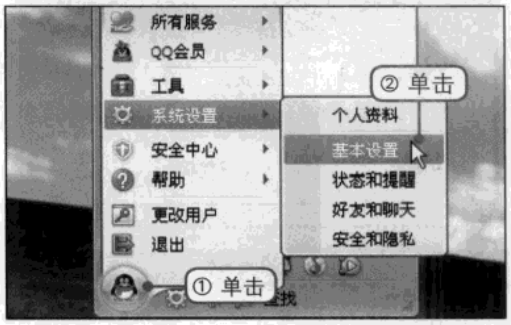


14.3.4 加密消息记录

用户保障了QQ聊天环境的安全之后，可启动消息记录加密对消息记录进行双重保护，以防他人偷窥聊天记录。

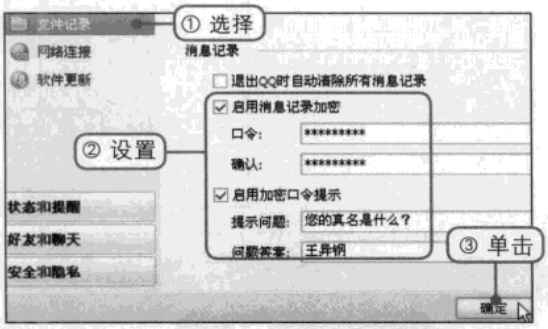
① 单击“基本设置”命令

登录QQ之后，①在主界面中单击“主菜单”按钮。②单击“系统工具>基本设置”命令。



② 设置消息加密口令和口令提示

打开“系统设置”对话框，①选择“文件记录”选项。②设置消息记录密码和口令提示。③单击“确定”按钮保存退出。



读书笔记

Chapter 15

电子邮件攻防

重点知识

1. 邮件病毒概述
2. 电子邮件炸弹攻防
3. 盗取电子邮箱密码的常用软件

随着科学技术及互联网的发展，电子邮箱逐渐取代了传统的通信方式，使用电子邮件写信并发送，只需花费很短的时间，就可将邮件传送到对方的电子邮箱里面，大大地节约了成本和时间。但是一些人通过非法的手段截取发送的电子邮件或者盗取用户的电子邮箱，严重影响了电子邮箱的安全和用户的隐私，因此必须做好电子邮箱的防范措施。

视频文件

参见随书光盘：视频教程\Chapter 15

Chapter 15 电子邮件攻防

15.2.2 使用Outlook Express拒绝垃圾邮件
15.2.3 使用E-mail Chomper防范电子邮箱炸弹
15.3.1 使用WebCracker获取Web邮箱密码
15.3.2 使用Fluxay探测电子邮箱密码

15.1 邮件病毒概述

使用电子邮件通信已经成为当今日常工作的主要通信模式。而病毒可通过各种手段进行传播，电子邮件也不例外，电子邮件病毒与普通的病毒是一样的，只是其传播途径主要是通过电子邮件来传播的。

15.1.1 认识邮件病毒

邮件病毒与普通的病毒没有什么区别，黑客使用它的目的也是为了入侵他人的电脑并成功地进行控制，使其成为“肉鸡”。所谓“肉鸡”，是指那些可以随意被黑客操控的电脑，黑客可以像操作自己的电脑那样来操作它们，而不被对方所发觉。

邮件病毒除了具有普通病毒的所有特点之外，还具有感染速度快、扩散范围广、破坏性大等特点。

1 感染速度快

在单机环境下，病毒只能通过U盘或者光盘等可移动设备从带有病毒的电脑传染到另一台电脑，但是在网络中可通过各种形式进行传播，例如通过电子邮件等网络通信机制进行迅速地传播。

2 扩散范围广

由于电子邮件是通过网络进行传播的，这直接使邮件病毒的扩散范围大大地扩大了，不但能在一瞬间传染整个局域网，还能在很短的时间之内将病毒传播到其他地方。

3 破坏性大

互联网中的电脑感染了电子邮件病毒之后，将会直接影响到网络的工作，轻则降低网络速度，影响工作的效率，重则将导致网络及电脑系统的崩溃，以及重要数据的丢失。

4 隐蔽性好

邮件病毒与普通的病毒相比更加隐蔽。一般来说，邮件病毒通常隐藏在邮件携带的附件中，或者是写邮件所使用的信纸中，这样不但加速了病毒的传播速度，也加大了查杀病毒的困难度。

5 不易被清除

单独的一台电脑遭受病毒后，可通过删除携带有病毒的文件或者格式化硬盘等方法清除病毒，但是如果电脑遭受了邮件病毒的入侵，则清除邮件病毒的难度将大大地增加，刚刚完成了清除工作的电脑很有可能由于网络中的另一台遭受邮件病毒入侵的电脑而感染，使得前面的清除工作成了无用功。

15.1.2 防范邮件病毒

若想防范邮件病毒，首先需要识别邮件病毒，用户可通过查看邮件携带的附件大小、邮件的地址和识别真伪退信三种方法来识别邮件病毒。

1 查看邮件携带的附件大小

电子邮件携带的附件通常是“邮件病毒”的最佳载体，用户可通过查看附件的大小来识别附件中是否带有邮件病毒。例如一个Word文档附件的大小一般为几十KB左右，一张普通的图片一般在50KB左右（由于照片的清晰度及所保存的格式不同，大小可能会有一定的差距），若邮件携带的附件大小远远超出了一般的大小范围，则很有可能该附件携带了邮件病毒。

2 查看邮件的地址

当用户无意中接收到陌生人发来的邮件时，一定要小心谨慎，在打开邮件之后，若该邮件中要求用户点击某一个网站链接或者下载某一个附件时，基本上可以断定该邮件携带有邮件病毒，直接将其彻底删除即可。

3 识别真伪退信

用户向好友发送邮件时，若写错了收信人的邮箱地址，则邮件服务器会自动将发送的邮件退回并提示用户确认邮箱地址是否正确，但是一些黑客通常会利用伪装的退信传播病毒。由于退回的邮件中通常有一个书写着用户邮件正文的附件，一旦用户打开伪装的邮件并查看附件后，邮件病毒就入侵到该电脑，用户若未及时发现，则会将该病毒传播到其他电脑中。识别真伪退信的方法很简单，只需要仔细确认一下邮件地址即可。

4 合理设置杀毒软件

现在市场上的一些杀毒软件虽然都具有邮件监控的功能，但还需要用户自己手动进行设置。例如用户使用瑞星杀毒软件则需要设置邮件监控中的发现病毒时的处理方式，建议用户设置为发现病毒时直接删除。

5 使用邮箱的反病毒功能

目前国内的一些邮箱服务器提供商都提供了邮箱的反病毒功能，凡是邮件或者邮件携带的附件中带有了病毒，系统会自动将其隔离或者删除，这样便可以安全地阅读邮件，不用担心电脑遭受邮件病毒的入侵。除此之外，用户在编写并发送邮件时邮箱的反病毒功能同样生效，这样用户便可放心地编写邮件以及上传附件。

6 谨慎对待邮件附件

当用户处理邮件携带的附件时，最好的方法是将其存放至电脑硬盘中，然后使用杀毒软件进行扫描，若没有发现病毒或者木马则可放心打开，若发现了则直接将其删除。

7 仔细选择邮件信纸

Fox Mail, Dream Mail等大部分邮件收发软件都提供了信纸模板，用户在写邮件时往往会选择漂亮的信纸，但是漂亮的信纸模板很有可能携带有邮件病毒。由于邮件管理软件中的信纸模板都是一些脚本文件，如果模板感染了如VBS/KJ、欢乐时光等脚本病毒时，使用该模板编写并发出的邮件同样携带有该病毒。因此用户不要盲目地使用邮件信纸，尽量少用，不要给邮件病毒任何传播的机会。

15.2 电子邮件炸弹攻防

电子邮件炸弹，英文名为E-mail Bomb，是黑客常用的攻击手段，其攻击方法简单、见效快。它实质上就是发送地址不详、容量庞大和充满了乱码的恶意邮件，也可称为大容量的垃圾邮件。由于电子邮件炸弹攻击是黑客在知道对方电子邮箱的前提下发送的，因此用户需谨慎公开自己的电子邮箱地址。

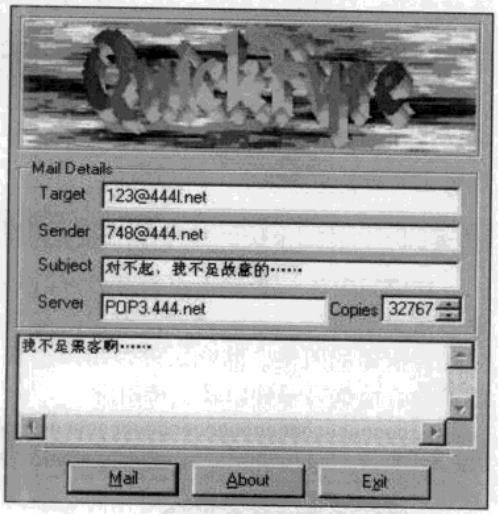
15.2.1 认识电子邮件炸弹

电子邮件炸弹是指发送那些自身体积（字节数）超过了信箱容量的电子邮件，或者由某服务器短时间内连续不断地向同一个信箱发送大量的电子邮件，将正常的邮件淹没在垃圾邮件的海洋中。由于现在使用的电子邮箱的大小一般都有限制，接收大量邮件将会导致信箱堵塞，从而使信箱打不开。

这种攻击手段不仅会干扰用户电子邮件系统的正常使用，甚至会影响到邮件系统所在的服务器系统的安全，造成整个服务器瘫痪，所以邮件炸弹也具有很大的危害。

现在已经有很多能自动产生邮件炸弹的程序，例如Quickfyre。

Quickfyre是一款可以同时发送大量的邮件的应用程序。其主界面如右图所示。



- 在Target文本框中输入收信人的信箱地址。
- 在Sender文本框中输入发信人的信箱地址。
- 在Subject文本框中输入邮件的主题。
- 在Server文本框中输入邮件服务器地址。
- 在Copies文本框中输入邮件复制的份数。

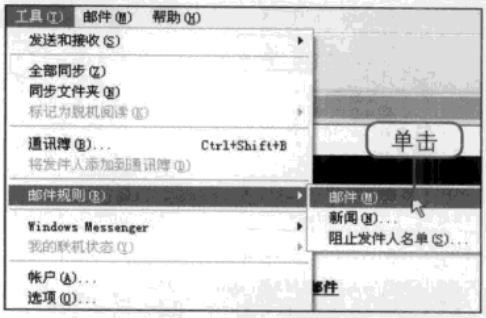
接着在主界面下方单击Mail按钮，该程序便开始连接服务器，连接成功之后便会发送大量的电子邮件到收信人的电子邮箱中。

15.2.2 使用Outlook Express拒绝垃圾邮件

Outlook Express是Windows操作系统自带的一款邮件收发软件，因此这里以Outlook Express为例，通过设置其邮件规则来拒绝垃圾邮件，防止电子邮件炸弹的攻击，更好地保护电子邮箱。

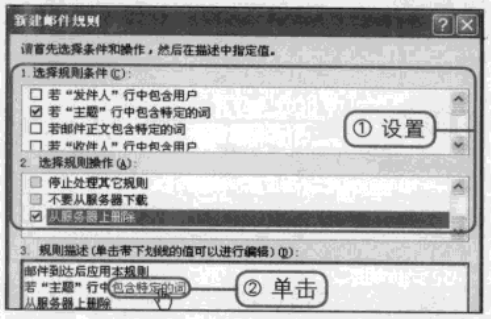
① 打开“新建邮件规则”对话框

打开Outlook Express主界面窗口，单击菜单栏中的“工具>邮件规则>邮件”命令。



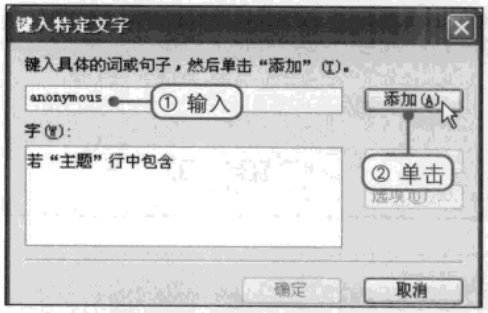
② 设置新建邮件规则

打开“新建邮件规则”对话框，①设置规则条件和规则操作分别为“若‘主题’行中包含特定的词”和“从服务器上删除”。②单击“包含特定的词”文字链接。



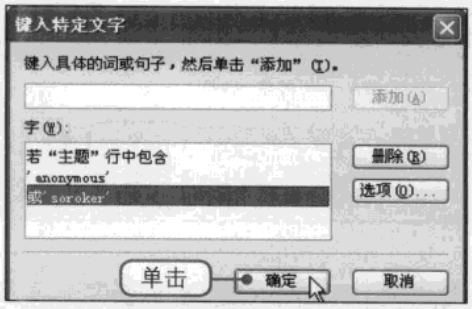
③ 键入特定文字

弹出“键入特定文字”对话框，①在文本框中输入特定的文字。②单击“添加”按钮。



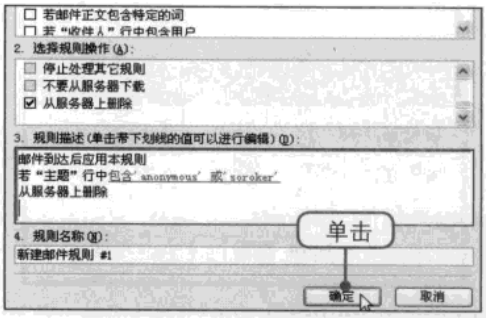
④ 返回“新建邮件规则”对话框

此时可看见文字添加成功，用户可使用相同的方法继续添加，接着单击“确定”按钮。



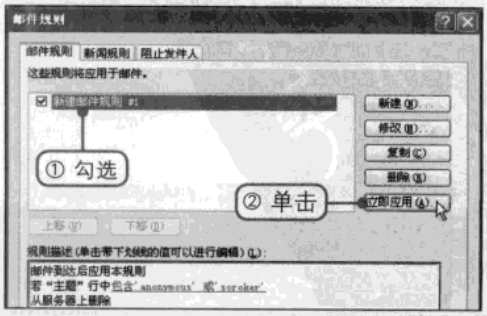
⑤ 确认添加的特定文字

返回“新建邮件规则”对话框，确认添加的特定文字正确无误后单击“确定”按钮。



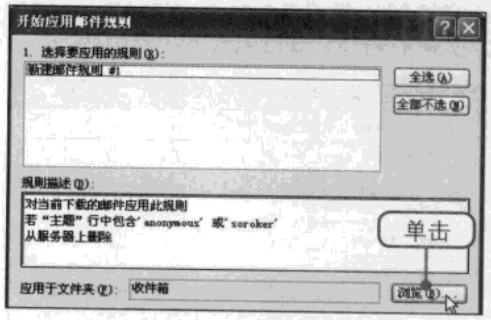
⑥ 打开“开始应用邮件规则”对话框

①在“邮件规则”对话框中勾选“新建邮件规则”复选框。②单击“立即应用”按钮。



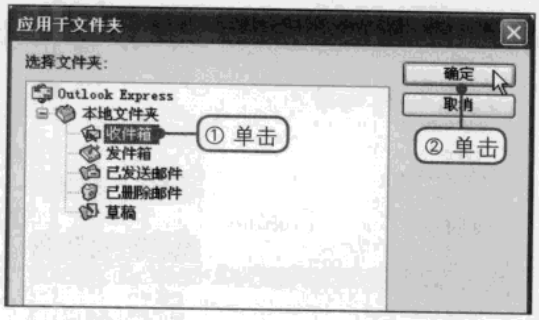
⑦ 打开“应用于文件夹”对话框

弹出“开始应用邮件规则”对话框，单击“应用于文件夹”选项中的“浏览”按钮。



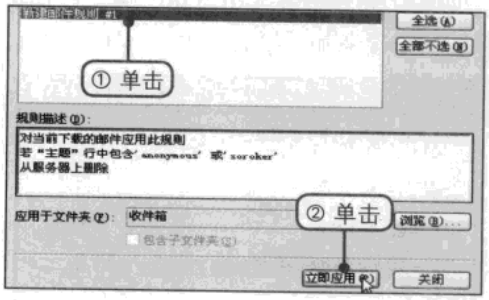
⑧ 选择应用的文件夹

弹出“应用于文件夹”对话框，①单击选中应用的文件夹。②单击“确定”按钮。



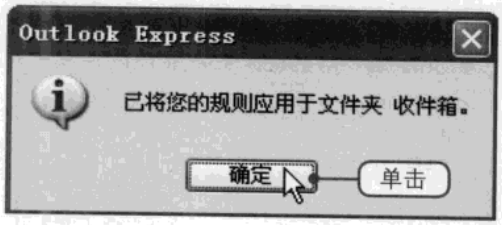
⑨ 单击“立即应用”按钮

返回“开始应用邮件规则”对话框，①单击“新建邮件规则”选项。②单击“立即应用”按钮。



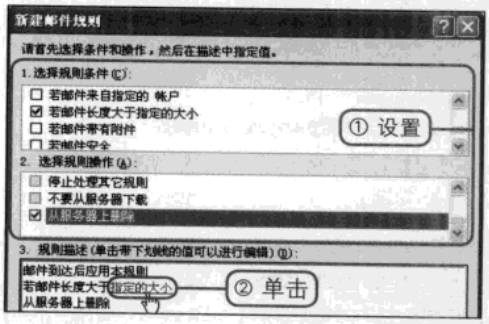
⑩ 应用成功

弹出提示用户已将邮件规则应用于文件夹收件箱的对话框，直接单击“确定”按钮返回“新建邮件规则”对话框。



⑪ 继续设置新建邮件规则

①继续设置规则条件和规则操作分别为“若邮件长度大于指定的大小”和“从服务器上删除”。②单击“指定的大小”文字链接。



⑫ 设置邮件大小的最大值

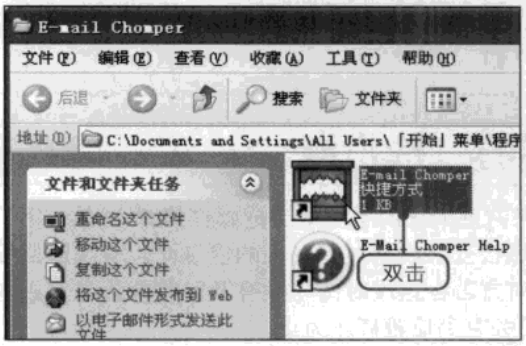
弹出“设置大小”对话框，①在“大小”微调框中设置邮件大小的最大值。②单击“确定”按钮保存退出即可。

15.2.3 使用E-mail Chomper防范电子邮件炸弹

E-mail Chomper是一款提供远程邮箱功能的应用软件，利用该软件可以在不用下载邮件内容的情况下列举出服务器上每封邮件的标题、寄信人以及附加文件的大小，当用户发现一些陌生人发送的邮件和附件是电子邮件炸弹时，便可直接将其删除，以有效地对付垃圾邮件和巨型邮件的进攻。从网上下载并安装该软件之后不会在桌面上出现对应的快捷图标。

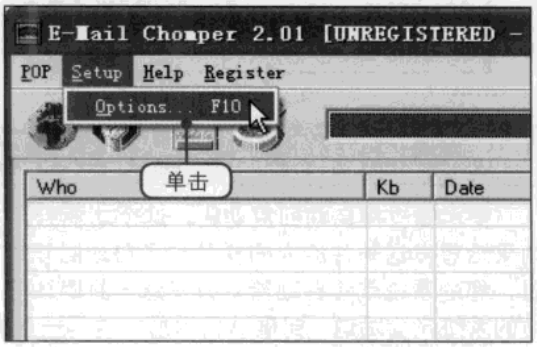
① 启动E-mail Chomper

下载并安装好E-mail Chomper软件之后会自动弹出“E-mail Chomper”窗口，在窗口中双击对应的快捷图标。



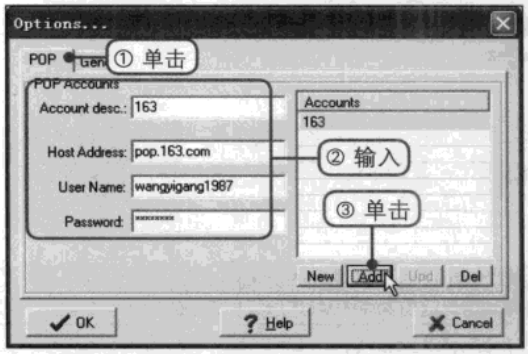
② 打开Options对话框

打开E-mail Chomper主界面窗口，在窗口的菜单栏中单击Setup>Options命令，打开Options对话框。



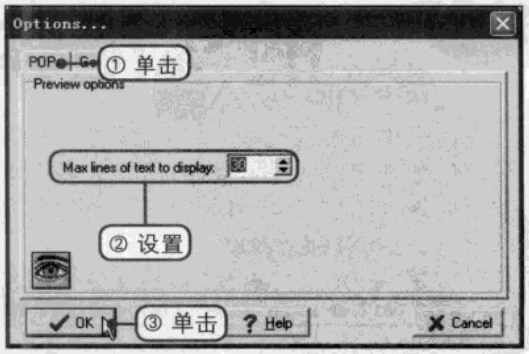
③ 设置POP选项

①单击POP标签切换至该选项卡，②填写远程管理的邮件服务器的地址（Account desc.）、主机地址（Host Address）、邮箱的用户名（User Name）和密码（Password），③单击Add按钮。



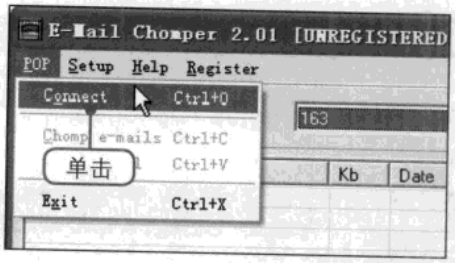
④ 设置View选项

①单击View标签切换至该选项卡。②在对话框中设置显示邮件的最大值，例如设置最大值为30。③单击OK按钮返回主界面窗口。



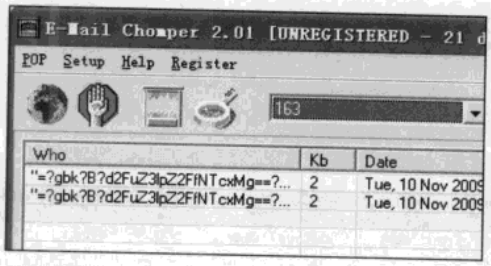
⑤ 单击Connect命令

在窗口的菜单栏中单击POP>Connect命令。



⑥ 查看邮件的详细信息

连接成功之后该软件自动下载电子邮箱中的邮件，用户可在窗口中查看邮件的详细信息，若发现一些垃圾邮件或者巨型邮件，直接删除即可。注意接收的邮件数量不要超过显示邮件的最大值。



15.2.4 避免电子邮件炸弹的一些措施

要尽量少用自动回复功能，这个功能给用户带来方便的同时也可能造成邮件炸弹.试想一下，如果给您发送邮件的人同样开启了自动回复功能，那么当您收到对方发来的信息而没有及时回复时，您的系统就会自动给对方发送一封确认信，而对方若在这段时间内没有及时收取信息，则对方的系统又会发送一封确认信给您，这样一直发送下去直到信箱撑爆为止。

学会伪装邮件地址，平时在公告板或论坛上发信息时，系统有可能需要用户提供自己的邮件地址，而垃圾邮件制造者会用一些专门的邮件地址搜集程序来搜集有效的邮件地址，所以当用户向公告板或论坛发送信息时都必须加倍小心，可在地址中添加一些文字，使自动搜集程序无法识别您的邮箱地址，而其他人却可轻易识别出。例如your_name防@yourisp垃圾.com，其中用户名和域名使自动搜集程序毫无用处，这样别人就不能获取您的邮箱地址，也就无法给您发送垃圾邮件了。

15.3 盗取电子邮箱密码的常用软件

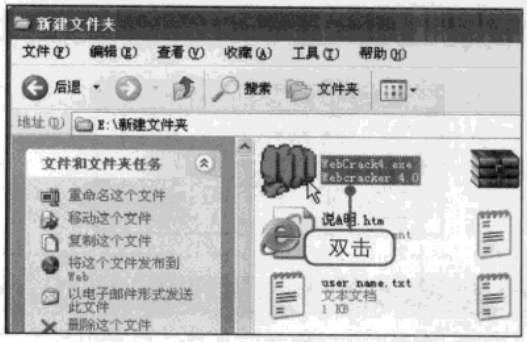
由于电子邮箱系统自身的漏洞，一些黑客便利用这些漏洞来盗取用户电子邮箱的密码，例如常用的WebCracker、流光等软件均可用来探测用户的电子邮箱漏洞，探测出漏洞之后便可通过各种手段来盗取其账号和密码。

15.3.1 使用WebCracker获取Web邮箱密码

黑客使用WebCracker破解用户的Web邮箱密码需要准备好账号字典、密码字典以及目标主机的地址。除此之外，该软件具有声音提示功能，能提醒探索结果是否成功。

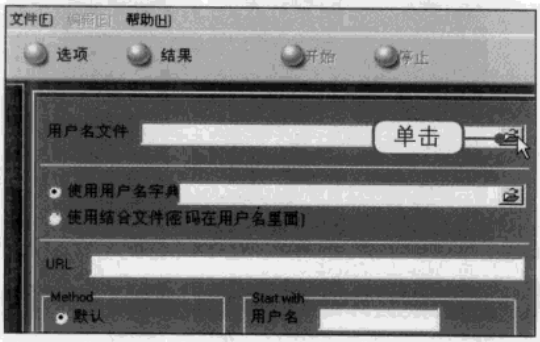
① 启动WebCracker

下载该软件后解压到磁盘分区中后，双击对应的快捷图标启动WebCracker。



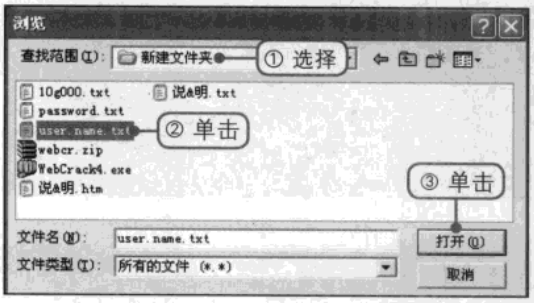
② 设置用户名文件

打开WebCracker主界面窗口，单击“用户名文件”文本框右侧的按钮。



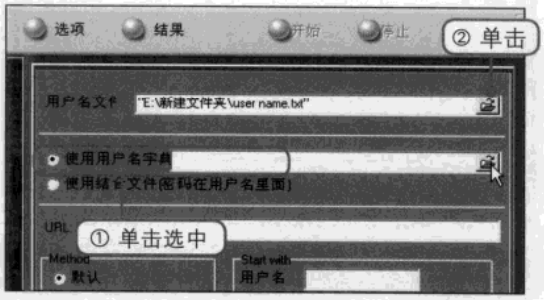
③ 选择账户字典

打开浏览对话框，①在“查找范围”下拉列表中选择路径。②单击选中账号字典。③单击“打开”按钮。



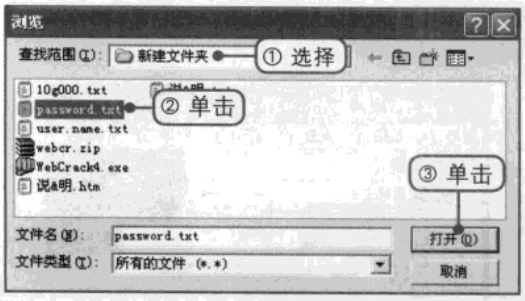
④ 设置用户名字典

返回主界面窗口，①单击选中“使用用户名字典”单选按钮。②单击文本框右侧的按钮。



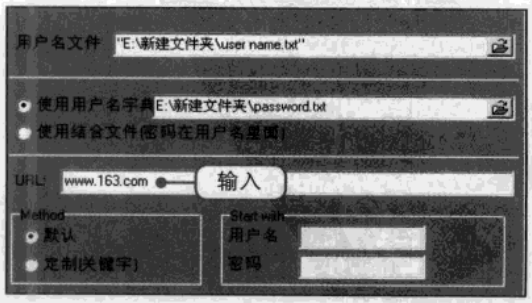
⑤ 选择密码字典

打开“浏览”对话框，①在“查找范围”下拉列表中选择路径。②单击选中密码字典。③单击“打开”按钮。



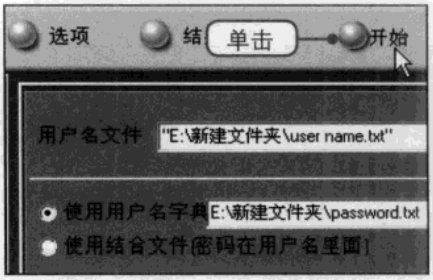
⑥ 输入URL地址

返回主界面窗口，在URL文本框中输入需要破解的网址或者URL地址，例如输入www.163.com。



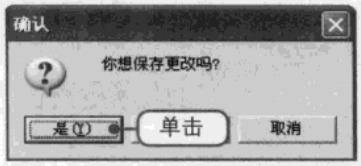
⑦ 单击“开始”按钮

在主界面窗口的顶部单击“开始”按钮。



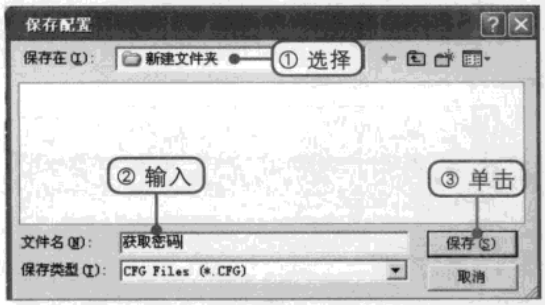
⑧ 保存更改设置

弹出确认对话框，提示用户是否保存更改设置，单击是按钮确认保存。



⑨ 设置保存路径和文件名

弹出保存配置对话框，①在“保存在”下拉列表中选择保存路径。②在“文件名”文本框中输入文件名。③单击“保存”按钮。



⑩ 开始探测

此时WebCracker开始探测，探测过程完全取决于账号字典和密码字典，这种方法属于暴力破解，请耐心等待。

15.3.2 使用Fluxay探测电子邮箱密码

Fluxay是一款国产软件，黑客有时利用该软件探测主机漏洞、用户信号以及破解用户的各种密码，包括电子邮箱密码。

① 启动Fluxay

下载并安装好Fluxay软件后会在桌面上出现对应的快捷图标，双击该图标启动Fluxay，打开其主界面窗口。

② 添加POP3主机

①右击窗口左侧的“POP3主机”选项。②在弹出的快捷菜单中单击“编辑>添加”命令。

③ 输入添加的主机名

弹出“添加主机（POP3）”对话框，①在文本框中输入添加的主机名，例如输入pop.163.com。②单击“确定”按钮。

④ 添加163用户

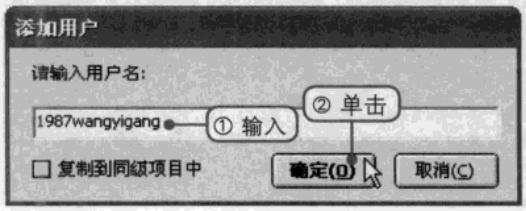
返回主界面窗口，①右击pop.163.com选项。②在弹出的快捷菜单中单击“编辑>添加”命令。

探测多个电子邮箱

若只想探测单独的一个邮箱，可按照以下的方法添加所要探测的电子邮箱的账户名即可。也可使用该软件一次性探测多个电子邮箱，具体操作是在步骤4中弹出的快捷菜单中单击“编辑>从列表添加”命令，接着选中账户字典即可根据账户字典探测多个电子邮箱。

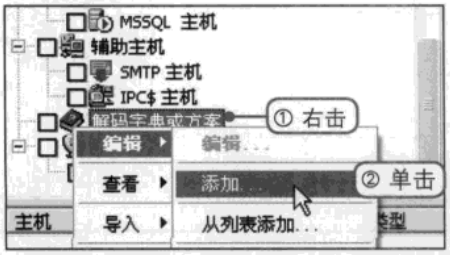
⑤ 输入用户名

弹出“添加用户”对话框，①在“请输入用户名”文本框中输入电子邮箱用户名。②单击“确定”按钮。



⑥ 添加解码字典或方案

返回主界面窗口，①向下拖动窗口左侧的滚动条，右击“解码字典或方案”选项。②在弹出的快捷菜单中单击“编辑>添加”命令。

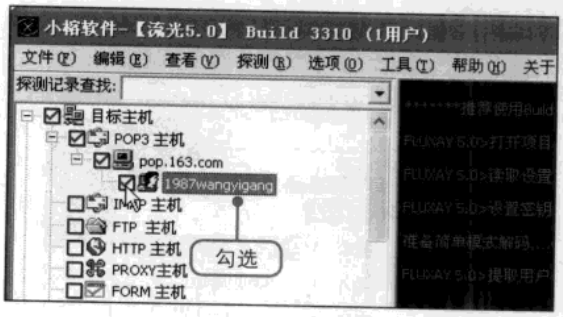


⑦ 选择密码字典

弹出“打开”对话框，①在“查找范围”下拉列表中选择密码字典所在的路径。②在下面的列表框中单击选中密码字典。③单击“打开”按钮。

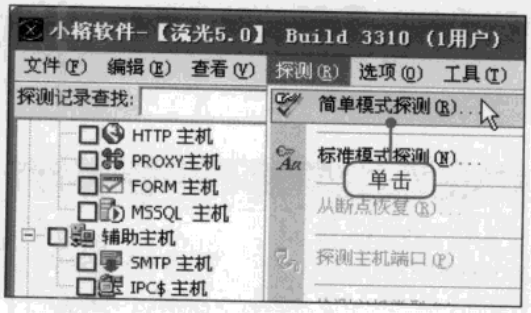
⑧ 选中电子邮箱

返回主界面窗口，向上拖动窗口中部的滚动条后勾选以电子邮箱用户名命名的复选框。



⑨ 简单模式探测

在窗口的菜单栏中单击“探测>简单模式探测”命令。



⑩ 开始探测

此时Fluxay正在根据账户名和密码进行探测，请耐心等待。

其他常用的破解软件

除了前面介绍的WebCracker和Fluxay软件能够探测电子邮箱的密码之外，网络中还有其他常用的破解软件，例如“溯雪Web密码探测器”、“黑雨”、“E-mail网页神抓”等软件。

读书笔记